

Kaseya 2

Standard Solution Package

Benutzerhandbuch

Versión 7.0

Deutsch

September 15, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

Kapitel 1

Einführung

In diesem Kapitel

Überblick

Beim **Standard Solution Package** handelt es sich um einen Satz von Datenobjekten, die in ihrer Gesamtheit als **Inhalte** bezeichnet werden, und bereits vorab in VSA geladen wurden. Kaseya hat diese Inhalte so definiert, dass sie Best-Practice-Lösungen für die Rechnerverwaltung innerhalb einer Kundenumgebung widerspiegeln. Die Inhalte sollen – ebenso wie Produktdokumentationen und Vorgehensweisen – Kaseya-Administratoren dabei helfen, direkt nach der Bereitstellung von Agents schnell und konsequent eine Reihe von empfohlenen Standardkonfigurationslösungen anzuwenden.

Features & Funktionen

Zu den Features und Funktionen zählen die optimierte Benutzerfreundlichkeit des Produkts, Audit & Inventarisierung, Remote-Support, Patch-Verwaltung, Monitoring & Benachrichtigungen, Richtlinien, Automatisierung, Reporting und vieles mehr.

Unterstützte Module

Dieses Paket bietet Inhalte und Support für die Kaseya K2 (Version 6.3)-Kernmodule/-Features wie z. B. System, Agent, Audit, Remote Control (inklusive Live-Connect), Patch-Verwaltung, Monitoring, Skriptings, Infocenter, Ansichten und Richtlinien-Verwaltung.

Unterstützte Betriebssystemplattformen und Software

Unterstützte Agent-Betriebssystemplattformen

Dieses Paket bietet Inhalte und Support für die folgenden Betriebssystemplattformen auf Agent-Rechnern.

- Microsoft Windows XP, 2003, 2003 R2, Vista, 2008, 2008 R2, 7, 2012
- Apple Macintosh Mac OS X 10.5 (Leopard), 10.6 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion)
- SuSE Linux Enterprise 10 und 11, Red Hat Enterprise Linux 5 und 6, Ubuntu 8.04 und höher, sowie OpenSuSE 11, CentOS 5 & 6

Unterstützte Systeme von Drittanbietern

Das ITSM-SS bietet Inhalte und Support für die folgenden Systeme und Anwendungen von Drittanbietern.

- E-Mail/Messaging
  - Exchange 2003, 2007, 2010, SMTP, IMAP, POP3, Blackberry Enterprise Server
- AntiVirus/Anti-Malware
  - Symantec AntiVirus Version 10, Corporate Edition Version 10, Endpoint Protection Version 11
  - McAfee VirusScan/Enterprise, Total Protection, Endpoint Protection
  - Sophos AntiVirus
  - Trend Micro OfficeScan Version 10, Worry-Free Business Security Version 11
  - AVG Technologies AntiVirus Version 8
  - Kaspersky Endpoint Security Version 8
  - Microsoft Security Essentials, Forefront Endpoint Protection
  - Integrierte Produkte für Drittanbieter-AV/AM aus dem Microsoft Security Center

- Backup/Wiederherstellung
  - Symantec Backup Exec Version 10/11/12/12.5/2010/2012
  - Computer Associates BrightStor ARCServe Backup Version 11.1/11.5/12/12.5/15
- Datenbankserver
  - Microsoft SQL Server 2005/2008/2008 R2
- Remotezugriff
  - Terminalserver, Citrix MetaFrame/Presentation Server/XenApp
- Netzwerkinfrastruktur
  - Microsoft Active Directory, Archivieren & Drucken, DHCP-Server, DNS-Server, FTP-Server
- Webserver
  - Microsoft IIS 6/7, SharePoint Server 2007/2010

Übersicht über das Paket

Die Inhalte des **Standard Solution Package** werden automatisch in VSA geladen. Manche der Inhalte sind nach **System-Cabinet** in einer Datenobjektstruktur organisiert. Hierzu zählen:

- **Richtlinien** – Richtlinien-Verwaltung > Richtlinien
- **Skripting** – Skripting > Erstellen/Planen
- **Monitorsets** – Monitoring > Monitorsets

Andere Inhalte wiederum werden in dedizierten Drop-down-Listen angezeigt:

- **Ansichten** – Es wird eine Liste vordefinierter *Ansichten* mit `zz[SYS]`-Präfix angezeigt, wenn Sie auf einer beliebigen Rechnerseite, auf der der Rechner-ID-/Gruppen-ID-Filter angezeigt wird, oben die Drop-down-Liste **Ansicht** auswählen.
- **Patch-Verwaltungsrichtlinien** – Es wird eine Liste vordefinierter *Genehmigungs- und Ablehnungsrichtlinien für die Patch-Verwaltung* mit `zz[SYS]`-Präfix angezeigt, wenn Sie die Drop-down-Liste **Patch-Verwaltung > Bestätigung gemäß Richtlinie > Richtlinie** auswählen.
- **Ereignis-Satz** – Es wird eine Liste vordefinierter *Ereignis-Sätze* mit `zz[SYS]`-Präfix angezeigt, wenn Sie die Drop-down-Liste **Monitoring > Ereignisprotokollwarnungen > Ereignisse definieren, die erfüllt oder ignoriert werden müssen** auswählen.

Fokus auf IT-Dienste

Das **Standard Solution Package** dient der Bereitstellung häufig benötigter IT-Dienste, die in der Regel von IT-Dienstanbietern oder IT-Supportunternehmen bereitgestellt werden. Zu diesen IT-Diensten gehören:

IT-Dienst	Beschreibung
Standardkonfiguration	Erleichtert die Verwaltung der Konfiguration sowie die Bereitstellung von Grundeinstellungen und Remote-Support-Benachrichtigungsrichtlinien.
Audit/Inventarisierung	Stellt aktuelle Hardware-/Softwarebestandsdaten für Rechner bereit.
Patch/Update-Management	Bietet Funktionen für das Patch/Update-Management zur Verbesserung der Stabilität, zur Verringerung von Sicherheitsrisiken und damit verbundenen Gefahren sowie für erhöhte Transparenz des Patch-Status von Rechnern.
Routinewartung	Sorgt für die routinemäßige Wartung von Rechnern, damit diese möglichst effizient arbeiten.
Monitoring	Sorgt für ein fortlaufendes Monitoring von Servern und/oder Arbeitsplatzrechnern in Hinblick auf Dienste, Performancedaten, Prozesse, Ereignisse, Integrität und Gesamtverfügbarkeit.
Reporting	Stellt Reportingfunktionen bereit, die Einblick in alle Aspekte der zahlreichen,

	bereitgestellten IT-Unterstützungsdienste bieten.

Automatische und spezialisierte Systemkonfiguration

Die bereitgestellten Inhalte eignen sich gleichermaßen für alle von Ihnen verwalteten Rechner. Bei den restlichen vordefinierten Inhalten handelt es sich um einen Katalog bekannter Alternativlösungen, die eventuell unter besonderen Umständen für Sie in Frage kommen.

- **Automatische Systemkonfiguration** – Innerhalb einer bestimmten Organisation häufig genutzte Inhalte können mithilfe des **Systems Management Configuration**-Setup-Assistenten schnell und automatisch konfiguriert werden. Folgen Sie hierzu einfach den im Abschnitt **System-Management-Konfiguration** *(siehe 6)* beschriebenen Schritten. Welche Inhalte durch den Assistenten verwendet werden, erfahren Sie im Abschnitt **Durch den Setup-Assistenten aktivierte Inhalte** *(siehe 19)*.
- **Spezialisierte Systemkonfiguration** – Nachdem Sie den **Systems Management Configuration**-Setup-Assistenten ausgeführt haben, können Sie Änderungen an den angewandten Richtlinien vornehmen. Sie haben die Möglichkeit, zusätzliche bzw. andere Inhalte oder Richtlinien auszuwählen und die ursprüngliche Konfiguration so anzupassen, das sie Ihren Bedürfnissen entspricht. Weitere Informationen zur individuellen Anpassung der Konfiguration finden Sie unter **Anpassen der Richtlinien einer Organisation** *(siehe 14)*. Im Abschnitt **Vollständiger Katalog aller Inhalte** *(siehe 65)* sind alle Ihnen zur Verfügung stehenden Inhalte beschrieben.

Kapitel 2

System-Management-Konfiguration

In diesem Kapitel

Der Setup-Assistent

Ab Version 6.3 beinhaltet Kaseya **Virtual System Administrator™** den **Systems Management Configuration**-Setup-Assistenten*.* Mit dem Einrichtungsassistenten können Sie schnell *Rechnerverwaltungsrichtlinien für eine bestimmte Organisation konfigurieren und anwenden.* Sind die Richtlinien konfiguriert, werden diese auf alle Rechner angewandt, die Sie im Auftrag der betreffenden Organisation verwalten. Richtlinien bestimmen viele verschiedene Aspekte der Rechnerverwaltung:

- Audit-Planung
- Monitoring
- Benachrichtigungen
- Patch-Verwaltung
- Rechner-Routinewartung mithilfe von Agentverfahren

Dank der Richtlinien müssen Sie nicht mehr jeden Rechner einzeln verwalten. Sie müssen nur eine Richtlinie zuweisen oder ändern. Eine Richtlinienzuweisung oder -änderung im Rahmen einer zugewiesenen Richtlinie wird innerhalb von 30 Minuten an alle beteiligten Rechner verteilt, ohne dass Sie in die Planung eingreifen müssen. Danach können Sie leicht feststellen, ob ein verwalteter Rechner die zugewiesenen Richtlinien erfüllt oder nicht. Die Verfolgung der Erfüllung jeder einzelnen Richtlinie liefert Ihnen die Informationen, die Sie für die zuverlässige Bereitstellung von IT-Diensten für die gesamte von Ihnen betreute Organisation benötigen.

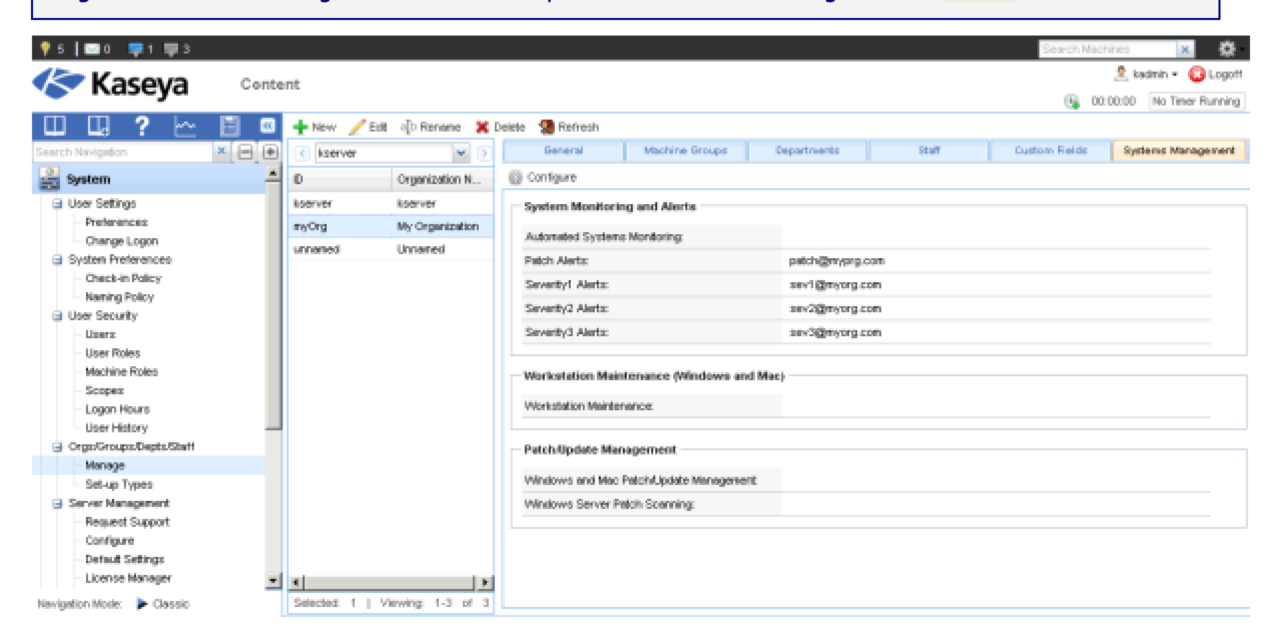
Beachten Sie die folgenden Hinweise, bevor Sie den **Systems Management Configuration**-Setup-Assistenten für eine Organisation ausführen.

- Sie können den **Systems Management Configuration**-Setup-Assistenten erneut ausführen, um für eine Organisation andere Optionen auszuwählen – allerdings nur unter der Voraussetzung, dass Sie in der **Policy Management** bisher keine individuellen Richtlinienzuweisungen für diese Organisation vorgenommen haben.
- Wenn Sie den **Systems Management Configuration**-Setup-Assistenten ausführen, bedeutet dies, dass Sie die Organisation *anhand von Richtlinien* verwalten möchten. Wenn Sie nach der Anwendung einer Richtlinie *manuell* Änderungen an Agent-Einstellungen vornehmen, wird die entsprechende Richtlinie überschrieben. Wenn Sie zum Beispiel Änderungen am Agent-Menü eines Rechners über die Seite **Agent-Menü** im **Agent**-Modul vornehmen, wird eine Überschreibbedingung für diesen Agent-Rechner erstellt. Überschriebene **Policy Management**-Richtlinien werden von da an ignoriert. Eine überschriebene Richtlinie kann zu jeder Zeit mithilfe des **Policy Management**-Moduls gelöscht werden.

Ausführen des Setup-Assistenten

1. Navigieren Sie zur Seite **System > Orgn./Gruppen/Abtlg./Personal > Verwalten**.
2. Wählen Sie im mittleren Fensterbereich eine Organisation aus.
3. Wählen Sie die Registerkarte **System-Management** aus.
4. Klicken Sie auf die Schaltfläche **Konfigurieren**.

Hinweis: In einem neuen VSA ohne installierte Agents werden Sie in der Benachrichtigungsleiste möglicherweise dazu aufgefordert, den Setup-Assistenten für die Organisation `myOrg` auszuführen.



In diesem Abschnitt

Setup-Assistent (Seite 1) – Systemüberwachung und Benachrichtigungen

- **Automatisches System-Monitoring aktivieren** – Wenn das System ein warnpflichtiges Element findet, erstellt es eine Benachrichtigung und benachrichtigt Sie per E-Mail.
- **Patch-Benachrichtigungen** – Die E-Mail-Adresse, die ausschließlich für Patch-Benachrichtigungs-E-Mails genutzt wird.

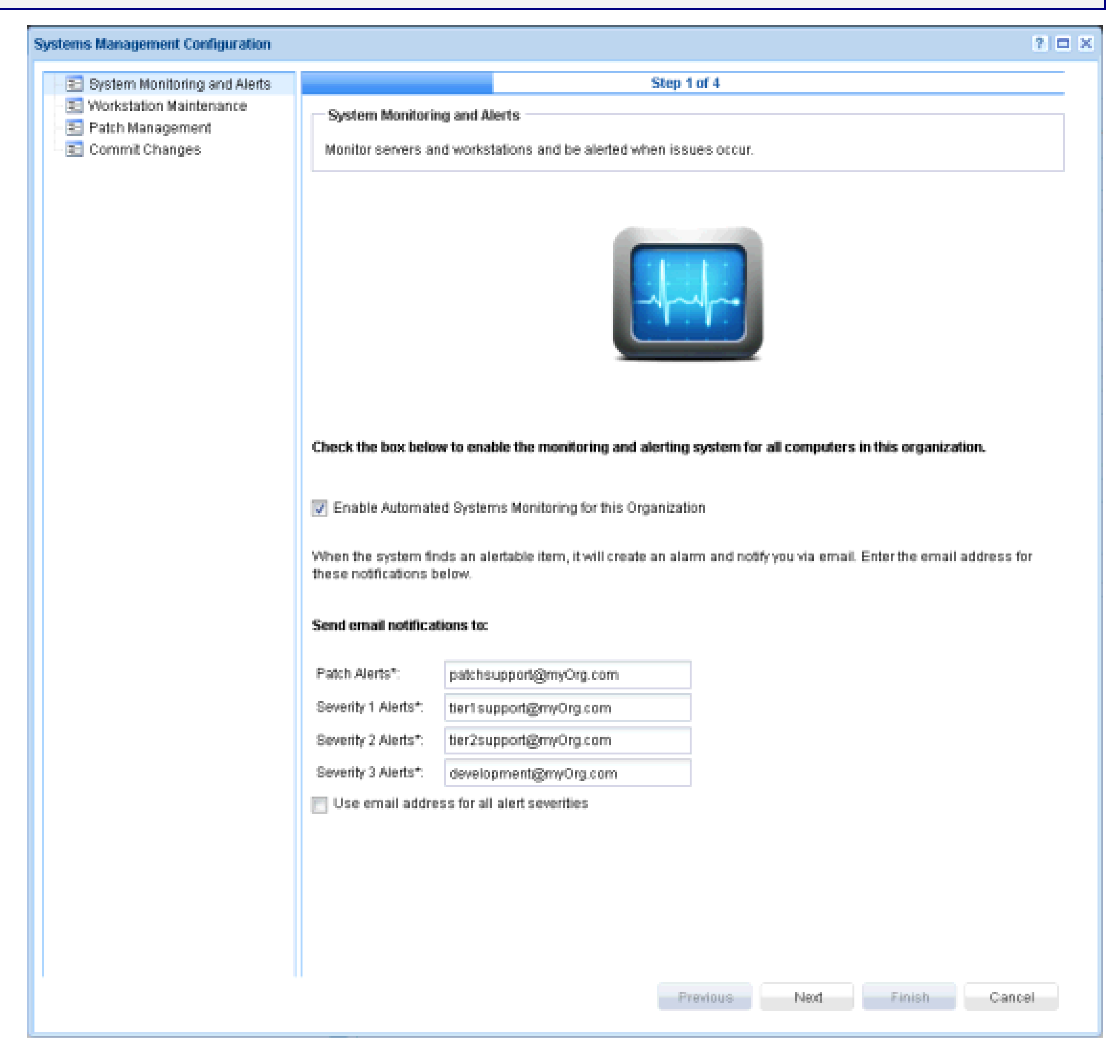
  Hinweis: Diese E-Mail-Adresse wird nur dann genutzt, wenn die Kontrollkästchen auf der Seite **Patch-Verwaltung** *(siehe 9)* des Assistenten aktiviert sind.

- **E-Mail-Adresse für alle Benachrichtigungen verwenden** – Deaktivieren Sie dieses Kontrollkästchen, um drei weitere Felder zur Eingabe von E-Mail-Adressen für *Benachrichtigungen unterschiedlicher Dringlichkeit* angezeigt zu bekommen. Aktivieren Sie das Kontrollkästchen, wenn Sie möchten, dass die E-Mail-Adresse im Feld **Patch-Benachrichtigungen** für alle vier Benachrichtigungsarten verwendet wird.

  Bei den Schweregrad-Benachrichtigungen handelt es sich um all diejenigen Benachrichtigungen, die *keine Patch-Benachrichtigungen sind.* Die Benachrichtigungen sind in verschiedene Dringlichkeitsstufen unterteilt, die Aufschluss darüber geben, wie kritisch der jeweilige Benachrichtigungszustand ist. Viele IT-Unternehmen verfügen über verschiedene Teams, von denen jedes für eine andere Dringlichkeitsstufe zuständig ist.

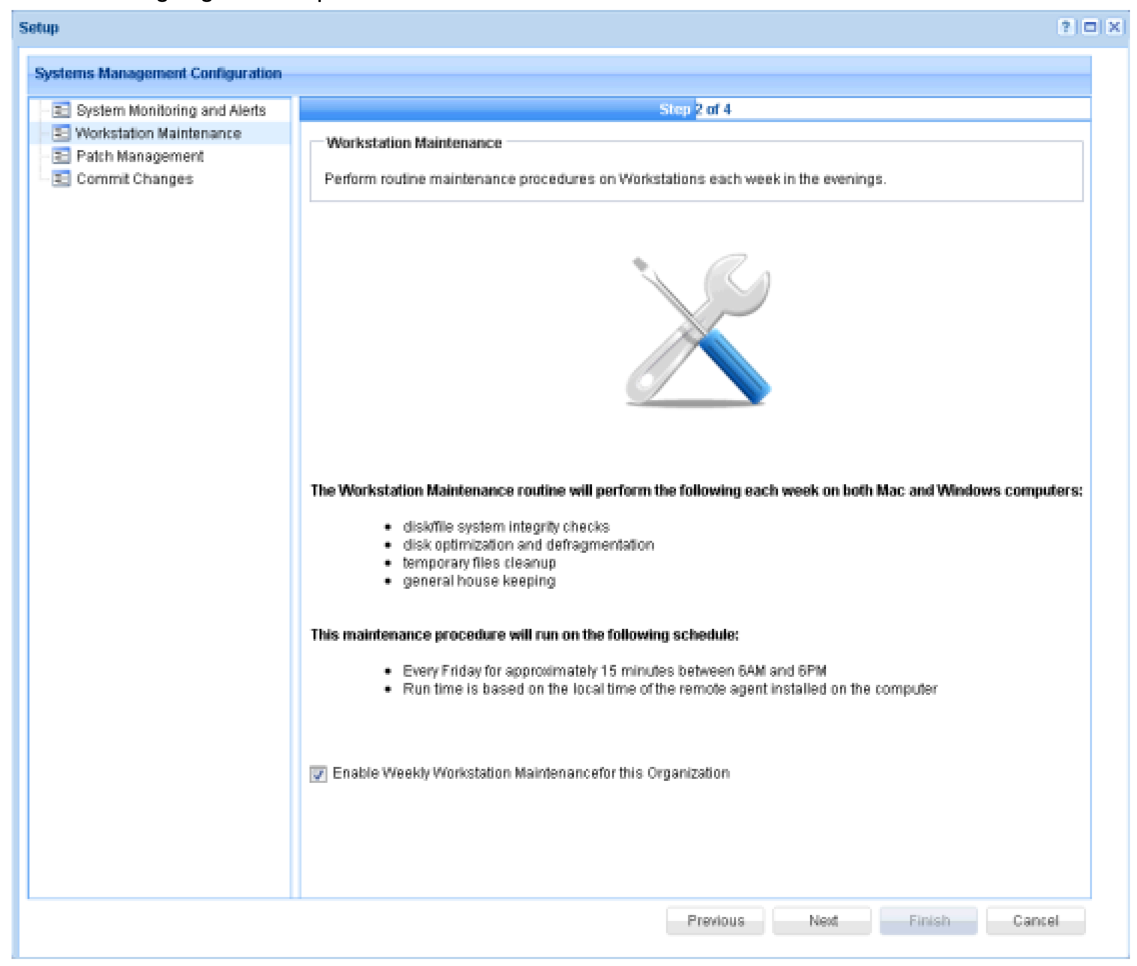
- **Benachrichtigungen der Dringlichkeitsstufe 1** – Die E-Mail-Adresse für weniger dringende Benachrichtigungen.
- **Benachrichtigungen der Dringlichkeitsstufe 2** – Die E-Mail-Adresse für relativ dringende Benachrichtigungen.
- **Benachrichtigungen der Dringlichkeitsstufe 3** – Die E-Mail-Adresse für äußerst dringende Benachrichtigungen.

Hinweis: Damit mehrere Organisationen die gleichen integrierten Standardrichtlinien in **Policy Management** nutzen können, werden Richtlinienfelder, die die Eingabe einer E-Mail-Adresse erfordern, mit **Platzhaltertoken** ausgefüllt. Bei den Token handelt es sich um `#patchAlertEmail#`, `#sev1AlertEmail#`, `#sev2AlertEmail#` und `#sev3AlertEmail#`. VSA ersetzt automatisch ein Token in einer Richtlinie durch die entsprechende E-Mail-Adresse für eine bestimmte Organisation, wenn eine Warnbenachrichtigung gesendet wird. Die E-Mail-Adressen der Organisation, für die die Token stehen sollen, sind auf dieser Seite des Assistenten anzugeben. Die **Policy Management**-Richtlinienkategorien, die E-Mail-Adressen enthalten, sind **Benachrichtigungen**, **Monitor-Sets** und **Patch-Einstellungen**.



Setup-Assistent (Seite 2) – Wartung von Arbeitsplatzrechnern

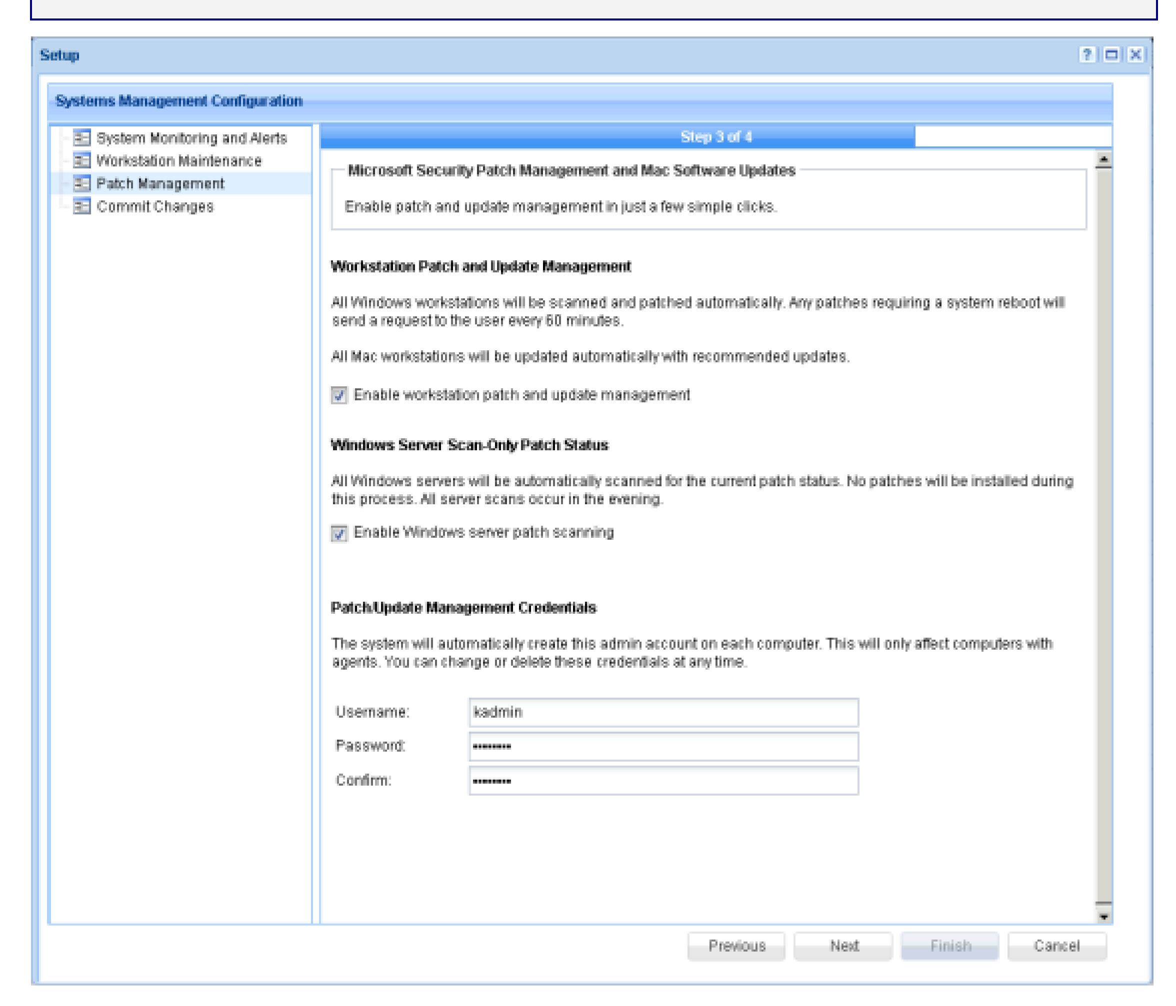
- **Wöchentliche Wartung von Arbeitsplatzrechnern aktivieren** – Ist diese Option aktiviert, wird einmal wöchentlich an einem Tag von Montag bis Freitag zwischen 18:00 und 06:00 Uhr eine Routinewartung der Arbeitsplatzrechner durchgeführt. Dies gilt nur für Windows- und Macintosh-Arbeitsplatzrechner, nicht jedoch für Linux-Arbeitsplatzrechner. Dazu gehören:
  - Überprüfung der Disk-/Dateisystemintegrität
  - Diskoptimierung und -defragmentierung
  - Bereinigung von temporären Dateien



Setup-Assistent (Seite 3) – Patch-Verwaltung

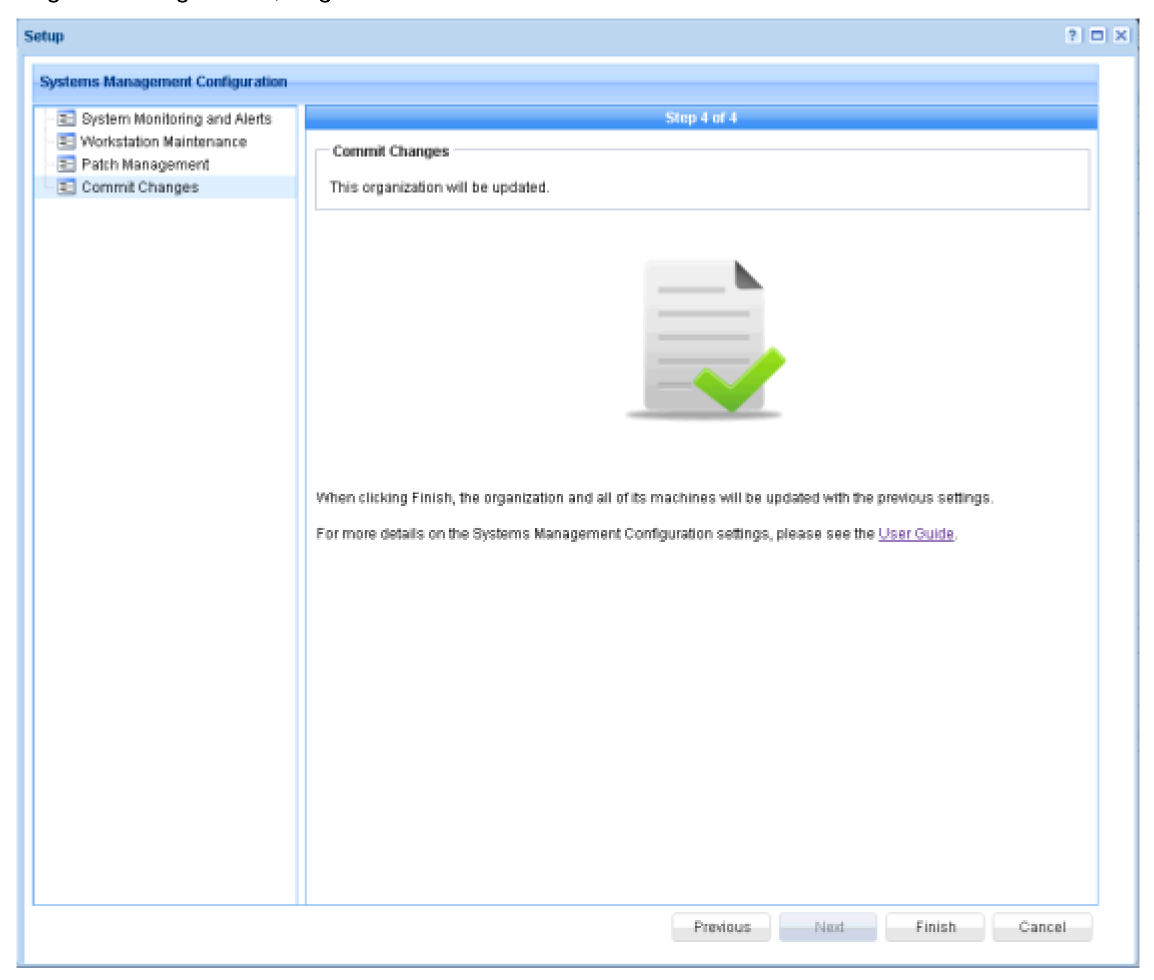
- **Patch- und-Update-Management für Arbeitsplatzrechner aktivieren** – Ist diese Option aktiviert, werden alle Windows-Arbeitsplatzrechner automatisch gescannt und gepatcht. Erfordert ein Patch einen Neustart des Rechners, wird der Benutzer alle 60 Minuten dazu aufgefordert, den Neustart zuzulassen.
- **Windows Server-Patch-Scanning aktivieren** – Es wird automatisch der aktuelle Status aller Windows-Server gescannt. Während dieses Vorganges werden keine Patches installiert. Alle Server-Scans finden abends statt. Das Patchen von Servern muss manuell durchgeführt werden.
- **Anmeldedaten für Patch-Verwaltung** – Das System erstellt automatisch auf jedem Computer dieses Administratorkonto. Das betrifft nur Computer mit Agents. Sie können diese Anmeldedaten jederzeit ändern oder löschen.

Hinweis: Anmeldedaten für dieses neue Konto werden der Seite ''Audit > Anmeldeinformationen verwalten'' für diese Organisation hinzugefügt. Die neuen Anmeldeinformationen erhalten den Status von Agent-Anmeldeinformationen; d. h. sie dienen als Agent-Anmeldeinformationen, wenn eine **Systems Management Configuration**-fähige Richtlinie für diese Organisation ausgeführt wird.



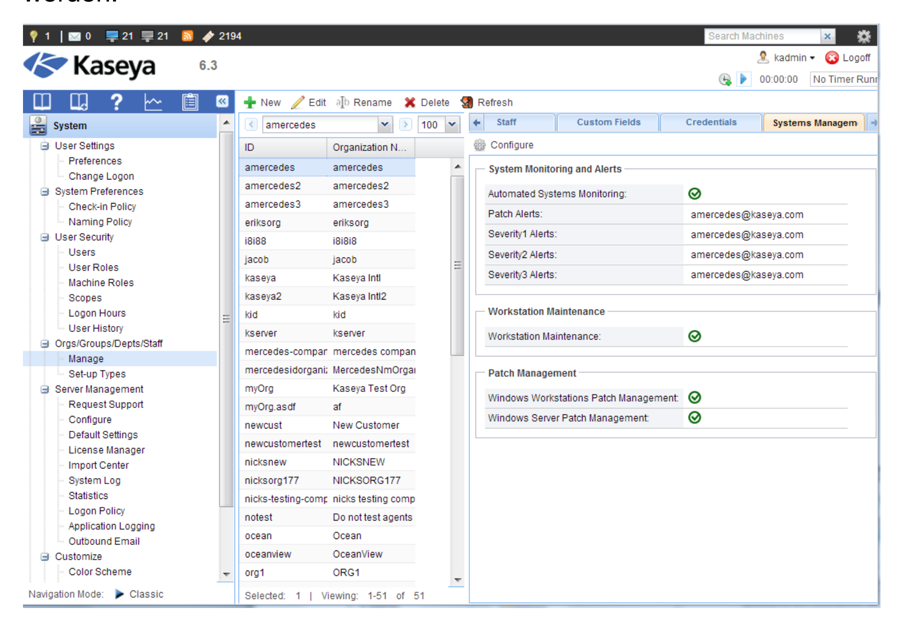
Setup-Assistent (Seite 4) – Abschluss der Konfiguration

Wenn Sie auf die Schaltfläche **Fertig stellen** klicken, erscheint ein Meldungsfeld, in dem bestätigt wird, dass Ihre Anfrage verarbeitet wird und dass dieser Vorgang bis zu fünf Minuten dauern kann. Es werden Richtlinien für die jeweilige Organisation erstellt und auf Systeme mit Agents, die zu dieser Organisation gehören, angewandt.



Bestätigung auf der Registerkarte "Systemverwaltung"

Nach dem Schließen des **Systems Management Configuration**-Setup-Assistenten kann es bis zu fünf Minuten dauern, bis Richtlinien auf verwaltete Rechner innerhalb der von Ihnen ausgewählten Organisation angewandt werden. Erst wenn dieser Vorgang abgeschlossen ist, sehen Sie in der Registerkarte **Systemverwaltung** grüne Kontrollkästchen zur Bestätigung, dass die von Ihnen ausgewählten Optionen übernommen worden sind. Es kann daraufhin 30 Minuten oder länger dauern, bis die angewandten Richtlinien auf die verwalteten Rechner in der Organisation übernommen werden.



Agents bereitstellen

Das Einzige, was nun noch zu tun bleibt, ist, einer Organisation verwaltete Rechner hinzuzufügen. Es gibt mehrere Möglichkeiten, Agents bereitzustellen.

- **Discovery** – Wenn Sie bereits mindestens einen Agent in einem Netzwerk installiert haben, empfiehlt sich die Ermittlung und Installation von Agents mithilfe des **Discovery-Moduls** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#7293.htm)*. Möglicherweise werden Sie in der Benachrichtigungsleiste dazu aufgefordert, eine Netzwerkermittlung durchzuführen, wenn ein neues Netzwerk ermittelt wurde.
- **Bereitstellung von Agents** – Wenn Sie den *ersten* Agent für ein neues Netzwerk bereitstellen, nutzen Sie dazu die Seite "Agent > **Agents bereitstellen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#491.htm)*". Eine Einführung in die Installation von Agents finden Sie im Schnellstarthandbuch **Agent-Bereitstellung** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_agentdeployment70.pdf#zoom=70&navpanes=0)*.

Bitte vergessen Sie nicht, dass sich mit dem **Systems Management Configuration**-Setup-Assistenten Richtlinien nur auf die Organisation anwenden lassen, die Sie ausgewählt haben. Stellen Sie daher sicher, dass die Agents, die Sie bereitstellen möchten, der gewünschten Organisation zugewiesen sind.

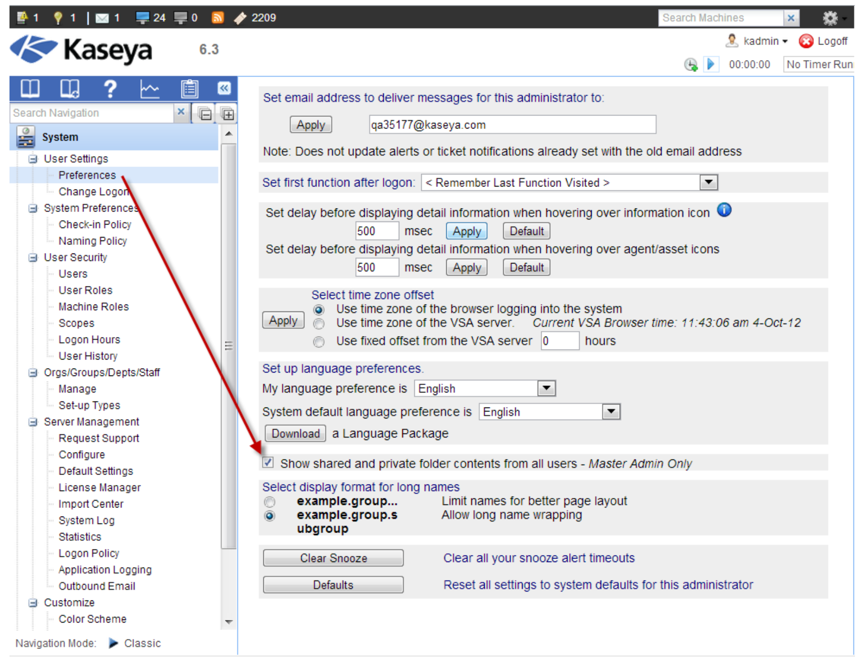
Funktionsweise:

Der Setup-Assistent *(siehe 6)* wurde lediglich die Funktionsweise des **Systems Management Configuration**-Setup-Assistenten erläutert. Wenn das alles war, was Sie wissen wollten, können Sie diesen Abschnitt hier überspringen. Wenn Sie aber gerne wissen würden, wie Sie mithilfe der **Systems Management Configuration** noch mehr aus VSA herausholen können, dann lesen Sie weiter.

In diesem Abschnitt

Voraussetzungen

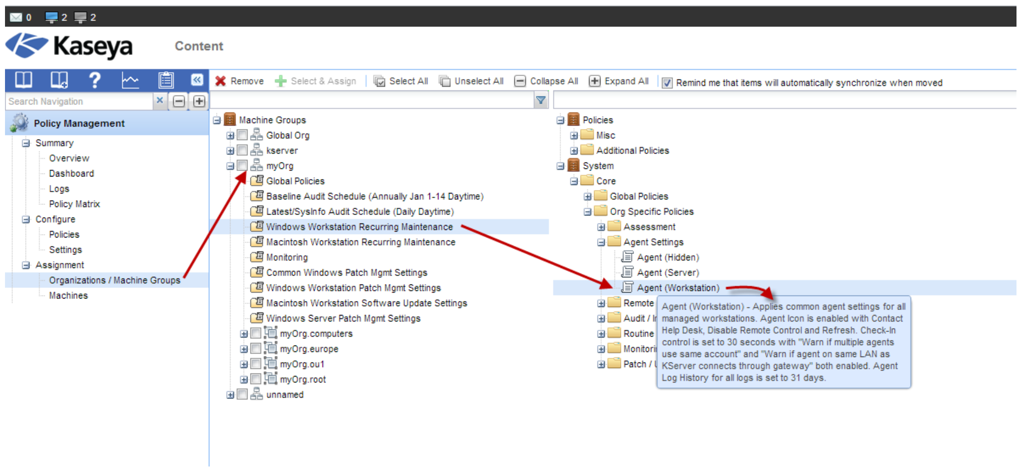
1. Stellen Sie sicher, dass Sie sich in VSA als *Hauptadministrator* (wenn Sie VSA vor Ort haben) bzw. als *Systemadministrator* (wenn sich VSA auf einer Cloud befindet) angemeldet haben. Dadurch stellen Sie sicher, dass Sie auf alle Features zugreifen können, von denen in diesem Abschnitt die Rede sein wird.
2. Stellen Sie sicher, dass das Kontrollkästchen **Freigegebene und private Ordnerinhalte aller Benutzer anzeigen – Nur Hauptadministrator** unter **System > Benutzereinstellungen > Voreinstellungen** aktiviert ist. Wenn Sie dieses Kontrollkästchen aktivieren, können Sie die in diesem Abschnitt beschriebenen System-Cabinet-Ordner einsehen.



Systemrichtlinien in der Richtlinien-Verwaltung

Entsprechend der Auswahl, die Sie im **Systems Management Configuration**-Setup-Assistenten getroffen haben, wird eine Liste von Richtlinien erstellt, die auf die von Ihnen ausgewählte Organisation angewendet wird. Sehen wir uns diese Richtlinien nun einmal genauer an.

1. Navigieren Sie zum Modul **Policy Management**.
2. Wählen Sie die Seite **Organisationen/Rechnergruppe** aus.
3. Erweitern Sie im mittleren Fensterbereich den Ordner der Organisation, die Sie beim Ausführen des **Systems Management Configuration**-Setup-Assistenten ausgewählt hatten.
4. Erweitern Sie das Cabinet **Systeme** im rechten Fensterbereich.



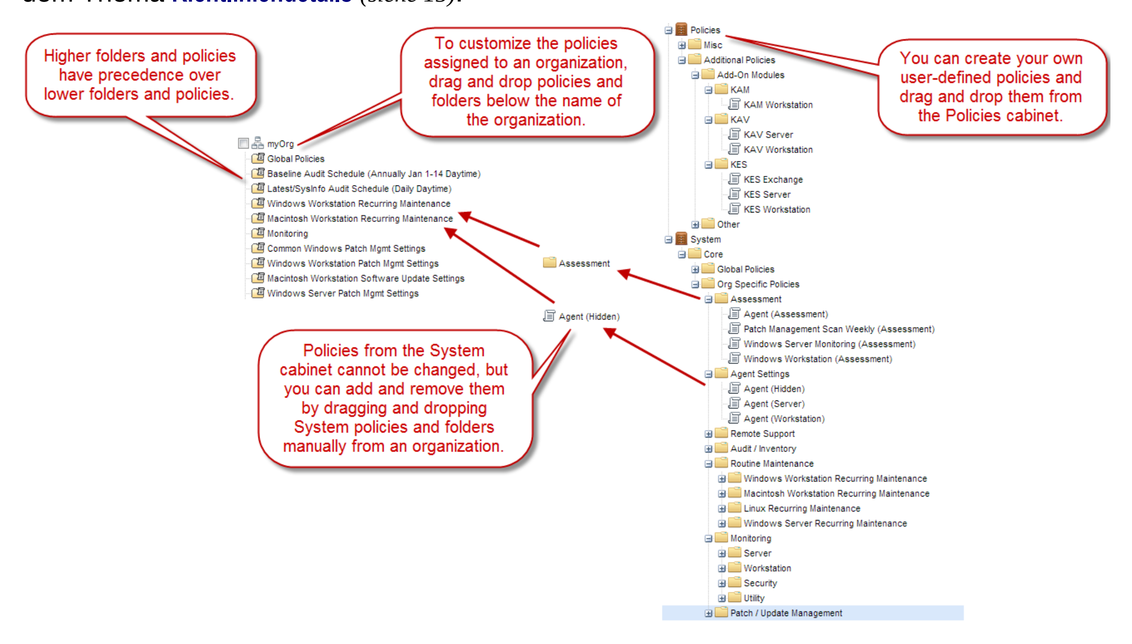
Beachten Sie, dass jedem Ordner, den Sie Ihrer Organisation zugewiesen haben, ein Ordner im rechten Fensterbereich entspricht. Dieser Ordner enthält in der Regel Unterordner sowie Richtliniensätze in den einzelnen Unterordnern. Halten Sie den Cursor über eine bestimmte Richtlinie, um eine Beschreibung dieser vordefinierten Richtlinie lesen zu können. Jeder verwaltete Rechner in der ausgewählten Organisation wird nun durch diese und alle weiteren Richtlinien, die dieser Organisation zugewiesen wurden, verwaltet.

Anpassen der Richtlinien einer Organisation

Auch wenn Sie nicht genau wissen, wie Richtlinien im Detail konfiguriert werden, können Sie die Richtlinien, die einer bestimmten Organisation zugewiesen sind, individuell anpassen.

Über die Seite **Policy Management > Organisationen/Rechnergruppe** können Sie die Richtlinien, die einer Organisation zugewiesen wurden, individuell anpassen, indem Sie Ordner oder Richtlinien per Drag & Drop in die Organisationsstruktur hinein- bzw. aus dieser herausziehen. Auf diese Weise können Sie auch Richtlinien aus dem System-Cabinet einer Organisation entfernen, falls Sie dies wünschen. Bitte beachten Sie, dass für die Abfolge der unter einer Organisation aufgelisteten Richtlinien **Richtlinienzuweisungsregeln** *(http://help.kaseya.com/webhelp/DE/KPM/7000000/index.asp#8140.htm)* gelten.

Zusätzliche Richtlinien und Ordner können per Drag & Drop entweder aus dem Cabinet "Systeme" oder aus dem Cabinet "Richtlinien" gezogen und abgelegt werden. System-Cabinet-Richtlinien können nicht verändert werden; es sind jedoch noch mehr System-Cabinet-Richtlinien verfügbar als diejenigen, die über den **Systems Management Configuration**-Setup-Assistenten ausgewählt wurden. Bevor Sie versuchen, Ihre eigenen benutzerdefinierten Richtlinien zu erstellen, sehen Sie noch einmal die verfügbaren System-Cabinet-Richtlinien durch. Im Abschnitt **Durch den Setup-Assistenten aktivierte Inhalte** *(siehe 19)* finden Sie eine Beschreibung aller System-Cabinet-Richtlinien. Detaillierte Informationen zum Aufbau einer Richtlinie finden Sie unter dem Thema **Richtliniendetails** *(siehe 15)*.

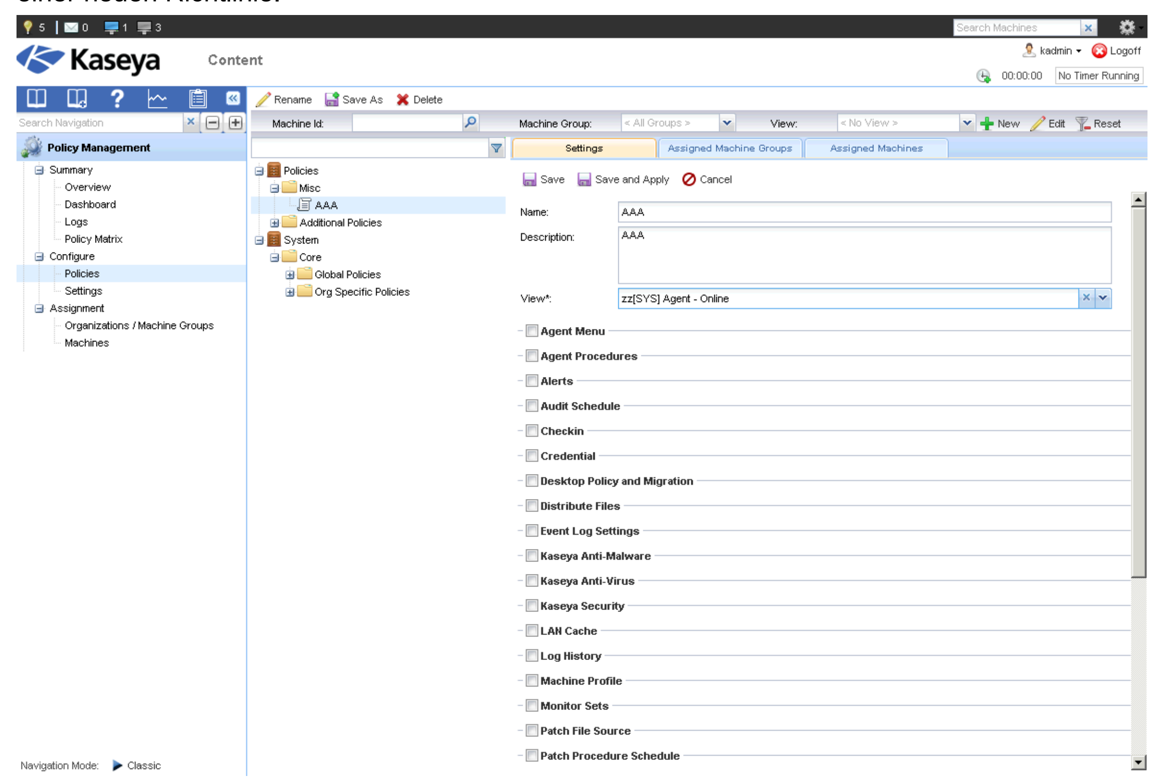


Richtliniendetails

> **Hinweis:** Die nächsten drei Themen geben einen groben Überblick über den Aufbau einer Richtlinie. Weitere Informationen über Richtlinien finden Sie in der **Policy Management -Online-Hilfe sowie im zugehörigen Benutzerhandbuch** *(http://help.kaseya.com/webhelp/DE/KPM/7000000/index.asp#8410.htm)*.

Details zu jeder Richtlinie – egal, ob es sich um eine Systemrichtlinie oder um eine benutzerdefinierte Richtlinie handelt – können Sie auf der Seite **Richtlinien** einsehen. Eine neue Richtlinie kann viele verschiedene Einstellungskategorien enthalten. So kann beispielsweise eine einzige Richtlinie zugleich für die Einstellung von Agent-Anmeldeeigenschaften, für die Festlegung eines Auditplans und für das Ausführen von Skripten verantwortlich sein.

Die folgende Abbildung zeigt eine Liste der verfügbaren Einstellungskategorien bei der Erstellung einer neuen Richtlinie.

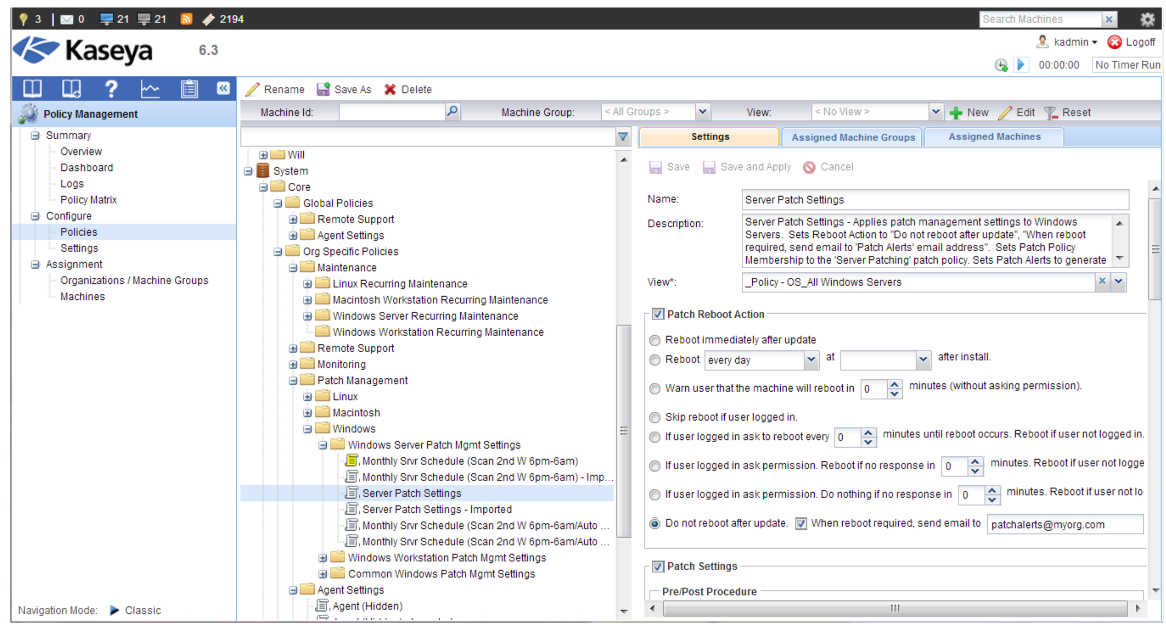


Integrierte Einstellungen vs. datenspezifische Einstellungen

Wenn Sie die Einstellungen in einer bestimmten Richtlinie prüfen oder konfigurieren, werden Ihnen zwei Arten von Einstellungen auffallen:

- **Integrierte Einstellungen** – Bei diesen Richtlinieneinstellungen handelt es sich in der Regel um Kontrollkästchen oder um Optionsfelder. Sie weisen die jeweilige Einstellung einem verwalteten Rechner zu; Sie müssen nichts weiter unternehmen.
- **Datenspezifische Einstellungen** – Diese Art von Richtlinieneinstellungen *legt ein Datenobjekt fest, das sich an einem anderen Ort in VSA befindet.* Dieses Datenobjekt ist entweder Teil der Standardinhalte, die vorab in VSA geladen wurden, oder es handelt sich um ein Datenobjekt, das ein anderer VSA-Benutzer erstellt hat und das dieser in Zusammenhang mit der Richtlinie verwendet.

In der folgenden Abbildung ist beispielsweise eine vordefinierte Systemrichtlinie zu sehen, die eine Richtlinie zum Neustarten eines Rechners nach einer Patch-Aktualisierung darstellt. Hierbei handelt es sich um eine *integrierte Einstellung*, für die Sie kein weiteres Datenobjekt angeben müssen. Die *datenspezifischen Einstellungen* werden im nächsten Thema behandelt.



Verknüpfung von Richtlinien mit Datenobjekten

Das Festlegen einer datenspezifischen Einstellung in einer Richtlinie erfordert, dass Sie ein Datenobjekt angeben, dass sich anderswo in VSA befindet.

Denken Sie daran, dass die System-Cabinet-Richtlinien in der **Policy Management** nur eine Art von *Standardinhalten* sind, die vorab in VSA geladen werden. Andere Arten von Inhalten sind:

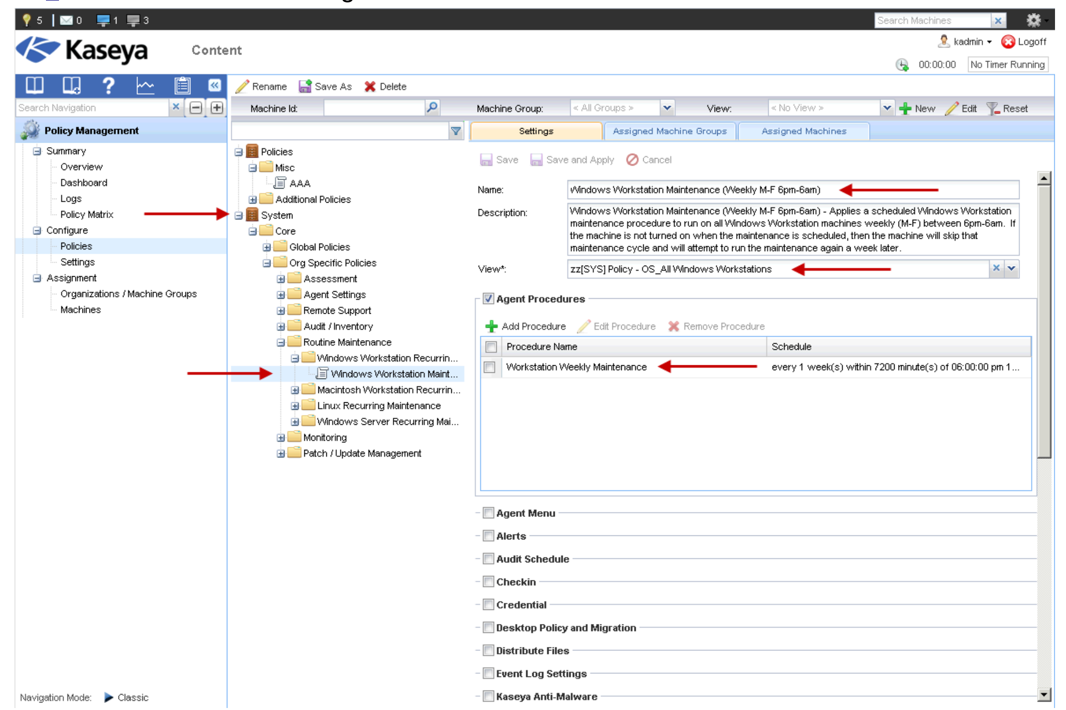
- Ansichten
- Patch-Richtlinien
- Ereignis-Sätze
- Monitor-Sets
- Skripting

Viele der automatischen Lösungen, die vom **Systems Management Configuration**-Setup-Assistenten bereitgestellt werden, werden aktiviert, indem man vordefinierte Systemrichtlinien mit diesen anderen Arten vordefinierter Systemdatenobjekten verknüpft.

In der untenstehenden Abbildung sehen Sie beispielsweise Details zu einer System-Cabinet-Richtlinie namens **Wartung von Windows-Arbeitsplatzrechnern (wöchentlich, Mo-Fr, zwischen 18:00 und 06:00 Uhr)**.

- Diese Richtlinie plant die wöchentlich Ausführung eines Skriptings namens **Wöchentliche Wartung von Arbeitsplatzrechnern**.

- Beachten Sie, dass diese Richtlinie auf Rechner beschränkt ist, die zur Ansicht **zz[SYS] Policy - OS_All Windows Workstations** gehören.



Dies ist nur ein Beispiel dafür, wie Systemrichtlinien mit Systeminhalten verknüpft werden, die sich anderswo in VSA befinden. Gehen Sie ebenso vor, wenn Sie die Einstellungen und Verknüpfungen anderer Richtlinien überprüfen möchten. Abgesehen von der Tatsache, dass Systemrichtlinien und -inhalte nicht verändert werden können, weist deren Konfiguration keinerlei Besonderheiten auf. Wenn Sie es also selbst versuchen möchten, erstellen Sie Ihre eigenen benutzerdefinierten Richtlinien und Inhalte und verknüpfen Sie diese so miteinander, wie Sie es hier sehen. Sie können auch mithilfe der Schaltfläche **Speichern unter** eine Kopie einer Systemrichtlinie erstellen und diese nach Ihren Vorstellungen und Bedürfnissen verändern.

> **Hinweis:** Weitere Informationen über Richtlinien finden Sie in der **Policy Management -Online-Hilfe sowie im zugehörigen Benutzerhandbuch** *(http://help.kaseya.com/webhelp/DE/KPM/7000000/index.asp#8410.htm).*

Kapitel 3

Durch den Setup-Assistenten aktivierte Inhalte

Die folgenden Kapitel geben einen Überblick über die Eigenschaften der Inhalte, die speziell für die Verwendung mit dem **Systems Management Configuration**-Setup-Assistenten entwickelt wurden. Diese Inhalte können im Übrigen auch manuell – ohne den Assistenten – verwendet werden.

In diesem Kapitel

Standardkonfiguration

Ziel

Das Ziel besteht in der Erleichterung der Verwaltung der Konfiguration sowie in der Bereitstellung von Grundeinstellungen und Remote-Support-Benachrichtigungsrichtlinien.

Überblick

Kaseya-Agents verfügen über eine Reihe von Konfigurationseinstellungen, die für alle verwalteten Rechner einheitlich sein sollten, so z. B. das Agent-Menü, die Eincheckkontrolle, das Arbeitsverzeichnis, die Anmeldedaten, die Protokollhistorie, die Ereignisprotokolleinstellungen und die Remote Control-Benachrichtigungsrichtlinien. Die Standardkonfiguration für Agents soll eine einheitliche, systemübergreifende Verwaltung dieser grundlegenden, systemweiten Konfigurationseinstellungen ermöglichen.

Richtlinien

Es wird ein Satz von Richtlinien bereitgestellt, die Standardkonfigurationseinstellungen für Agents auf alle Rechner innerhalb der unterstützten IT-Infrastruktur übertragen. Diese Richtlinien steuern auf der Grundlage eines allgemeinen Best-Practice-Anwendungsfalls für die Systemkonfiguration beispielsweise Einstellungen wie das Agent-Menü, die Eincheckkontrolle, das Arbeitsverzeichnis, die Anmeldedaten, die Protokollhistorie, die Ereignisprotokolleinstellungen und die Remote Control-Benachrichtigungsrichtlinien. Die Richtlinien befinden sich unter **[System].Core.Global Policies**, und werden nachfolgend beschrieben.

- **Agent-Einstellungen**
  - **Agent (Core)** – Überträgt die gebräuchlichsten Agent-Einstellungen auf alle verwalteten Rechner. Das Symbol "Agent" ist aktiviert, allerdings ist nur die Option "Aktualisieren" verfügbar. Die Eincheckkontrolle ist auf 30 Sekunden gesetzt, und die Optionen "Warnen, wenn mehrere Agents das gleiche Konto verwenden" und "Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist" sind aktiviert. Die Agent-Protokollhistorie ist für alle Protokolle auf 31 Tage gesetzt.
  - **Windows-Agent** – Überträgt Windows-spezifische Agent-Einstellungen auf die jeweiligen Arbeitsplatzrechner. Pfad für das Arbeitsverzeichnis: c:\kworking.
  - **Linux-Agent** – Überträgt Linux-spezifische Agent-Einstellungen auf die jeweiligen Arbeitsplatzrechner. Pfad für das Arbeitsverzeichnis: /tmp/kworking.
  - **Macintosh-Agent** – Überträgt Macintosh-spezifische Agent-Einstellungen auf die jeweiligen Arbeitsplatzrechner. Pfad für das Arbeitsverzeichnis: /Library/kworking.
- **Remote-Support**
  - **Server-RC-Benachrichtigungsrichtlinie (Automatisch mit Administratorhinweis)** – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Server. Benutzerbenachrichtigungstyp wird auf "Automatisch Kontrolle übernehmen" gesetzt, und die Option "Administratormitteilung für Start von Remote Control erforderlich" wird aktiviert.
  - **Arbeitsplatzrechner-RC-Benachrichtigungsrichtlinie (Benachrichtigung/Beendigung mit Administratorhinweis)** – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Arbeitsplatzrechner. Der Benutzerbenachrichtigungstyp wird auf "Benachrichtigung anzeigen, falls der Benutzer angemeldet ist‘ und "Benutzer benachrichtigen, wenn die Sitzung beendet ist" gesetzt, und die Option "Administratormitteilung für Start von Remote Control erforderlich" wird aktiviert.

Audit/Inventarisierung

Ziel

Das Ziel besteht darin, eine Routinestrategie für Audit und Inventarisierung bereitzustellen, durch die sich die Transparenz von Hardware- und Softwarebeständen erhalten lässt, um so die langfristige Planung, die Compliance, lang- und kurzfristige Projekte, die Entscheidungsfindung und die Fehlerbehebung zu erleichtern.

Überblick

Kaseya unterstützt zahlreiche Arten von Agent-basierten Audits zur Ermittlung von Hard- und Softwarekomponenten innerhalb einer IT-Infrastruktur. Diese Audits können in die Gruppen "Aktuell", "Basis" und "Systeminformationen" unterteilt werden. Audits des Typs "Aktuell" dienen dazu, die Informationen zur Hard- und Softwareausstattung von Rechnern stets aktuell zu halten. Audits des Typs "Basis" liefern Informationen zur Hard- und Softwareausstattung von Rechnern zu einem bestimmten Zeitpunkt. Audits des Typs "Systeminformationen" liefern mithilfe von SMBIOS zusätzliche Details zur Hardwareausstattung. Um die Informationen zu den einzelnen Rechnern stets aktuell zu halten und somit strategische und taktische Entscheidungen zu erleichtern oder gar erst zu ermöglichen, ist es wichtig, die genannten Audits in regelmäßigen Abständen durchzuführen. Die Audits liefern Informationen wie z. B. Bestandsdaten, mit deren Hilfe sich bestimmte Systemtypen leicht auffinden lassen sollten und dank derer ein effektives Reporting und Handeln in Bezug auf diese Rechnergruppen möglich sein sollte.

Richtlinien

Es wird ein Satz von Richtlinien zur Planung regelmäßig wiederkehrender Audits für alle Rechner innerhalb der unterstützten IT-Infrastruktur bereitgestellt. Diese Richtlinien ermöglichen das Sammeln wichtiger Anwendungsfalldaten für den Audit-/Inventarisierungsdienst. Die Richtlinien befinden sich unter **[System].Core.Org Specific Policies.Audit / Inventory**, und werden nachfolgend beschrieben.

- **Baseline.Baseline Audit Schedule (jährlich, 1.–14. Januar, tagsüber)**
  - **Basisauditplan (jährlich, 1.–14. Januar, 06:00–18:00/Energiemanagement** – Führt im Zeitraum vom 1. bis zum 14. Januar – jeweils zwischen 06:00 und 18:00 Uhr – auf allen bereitgestellten und eingecheckten Rechnern ein geplantes, jährliches Basis-Audit durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion, um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie kommt vor allem zum Einsatz, wenn jährliche Audits zu Planungs- oder Compliance-Zwecken erforderlich sind, und wenn für betriebliche Aufgaben ein Vergleich der Ergebnisse von "Basis"- und "Aktuell"-Audits benötigt wird. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.
- **Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (täglich, tagsüber)**
  - **Aktuell/SysInfo Auditplan (täglich, Mo-Fr, 06:00–18:00/Energiemanagement)** – Führt auf allen Rechnern, die täglich (Mo–Fr) zwischen 06:00 und 18:00 Uhr eingecheckt sind, Audits vom Typ "Aktuell" und "Systeminformationen" durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion, um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie kommt vor allem dann zum Einsatz, wenn Kunden werktags während der Arbeitszeit Audits durchführen müssen, da die Rechner in der Regel nachts und an den Wochenenden ausgeschaltet sind. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.

Ansichten

Es wird ein Satz vordefinierter Ansichten bereitgestellt, die in allen Bereichen der IT-Dienstverwaltung sowie zur Unterstützung des Audit-/Inventarisierungsdienstes eingesetzt werden können. Diese Ansichten bieten die Möglichkeit, die Rechner in einem System nach vorhandener Hardware und Software oder nach deren Rolle zu filtern. Die folgenden Ansichten können sowohl für

Reportingzwecke als auch für betriebliche Aktivitäten genutzt werden.

Ansichtsname	Beschreibung
zz[SYS] HW - Dell	Zeigt alle Rechner des Herstellers Dell an.
zz[SYS] HW - Dell PowerEdge	Zeigt alle Rechner des Herstellers Dell an, in deren Produktnamen "PowerEdge" vorkommt.
zz[SYS] HW - HP	Zeigt alle Rechner des Herstellers HP/Hewlett Packard an.
zz[SYS] HW - HP ProLiant	Zeigt alle Rechner des Herstellers HP/Hewlett Packard an, in deren Produktnamen "ProLiant" vorkommt.
zz[SYS] HW - IBM	Zeigt alle Rechner des Herstellers IBM an.
zz[SYS] HW - IBM Series X	Zeigt alle Rechner des Herstellers IBM an, in deren Produktnamen "Series X" vorkommt.
zz[SYS] HW - Lenovo	Zeigt alle Rechner des Herstellers Lenovo an.
zz[SYS] HW - Not Portable	Zeigt alle Rechner an, bei denen es sich nicht um tragbare Geräte handelt.
zz[SYS] HW - Portable	Zeigt alle Rechner an, bei denen es sich um tragbare Geräte (d. h. Notebooks, Laptops, tragbare PCs, Tablet-PCs, Handhelds, Subnotebooks oder Netbooks) handelt.
zz[SYS] HW - Under 1GB Memory	Zeigt alle Rechner mit weniger als 1 GB Speicher an.
zz[SYS] HW - Under 512MB Memory	Zeigt alle Rechner mit weniger als 512 MB Speicher an.
zz[SYS] HW - Virtual Guest	Zeigt alle Rechner an, bei denen es sich um virtualisierte Computer (VMWare-, XenServer-, VirtualBox- oder HyperV-Gäste) handelt.
zz[SYS] Network - 10.11.12.x	Zeigt Agents eines bestimmten 10.11.12.x-Netzwerks an.
zz[SYS] OS - All Linux	Zeigt alle Linux-Rechner an.
zz[SYS] OS - All Mac OS X	Zeigt alle Rechner mit Mac OS X an.
zz[SYS] OS - All Mac OS X Servers	Zeigt alle Mac OS X-Server an.
zz[SYS] OS - All Mac OS X Workstations	Zeigt alle Mac OS X-Arbeitsplatzrechner an.
zz[SYS] OS - All Servers	Zeigt alle Rechner mit Serverbetriebssystem an.
zz[SYS] OS - All Windows	Zeigt alle Windows-Rechner an.
zz[SYS] OS - All Windows SBS	Zeigt alle Windows SBS-Server an.
zz[SYS] OS - All Windows Servers	Zeigt alle Windows-Server an.
zz[SYS] OS - All Windows Workstations	Zeigt alle Windows-Arbeitsplatzrechner an.
zz[SYS] OS - All Workstations	Zeigt alle Rechner mit einem Betriebssystem für Arbeitsplatzrechner an.
zz[SYS] OS - Mac OS X 10.5 Leopard	Zeigt alle Rechner mit Mac OS X 10.5 an.
zz[SYS] OS - Mac OS X 10.6 Snow Leopard	Zeigt alle Rechner mit Mac OS X 10.6 an.
zz[SYS] OS - Mac OS X 10.7 Lion	Zeigt alle Rechner mit Mac OS X 10.7 an.
zz[SYS] OS - Mac OS X 10.8 Mountain Lion	Zeigt alle Rechner mit Mac OS X 10.8 an.
zz[SYS] OS - Win 2003 SBS	Zeigt alle Rechner mit dem Betriebssystem Windows 2003 Small Business Server (SBS) an.
zz[SYS] OS - Win 2003 Server	Zeigt alle Rechner mit dem Betriebssystem Windows 2003 Server an.
zz[SYS] OS - Win 2008 R2 Server	Zeigt alle Rechner mit dem Betriebssystem Windows 2008 Server R2 an.
zz[SYS] OS - Win 2008 SBS	Zeigt alle Rechner mit dem Betriebssystem Windows 2008 Small Business Server an.
zz[SYS] OS - Win 2008 Server	Zeigt alle Rechner mit dem Betriebssystem Windows 2008 Server an.

zz[SYS] OS - Win 2012 Server	Zeigt alle Rechner mit dem Betriebssystem Windows 2012 Server an.
zz[SYS] OS - Win 7	Zeigt alle Rechner mit dem Betriebssystem Windows 7 an.
zz[SYS] OS - Win Vista	Zeigt alle Rechner mit dem Betriebssystem Windows Vista an.
zz[SYS] OS - Win XP	Zeigt alle Rechner mit dem Betriebssystem Windows XP an.
zz[SYS] Role - BackupExec Server	Zeit alle BackupExec-Server an.
zz[SYS] Role - Blackberry Server	Zeigt alle Blackberry Enterprise-Server an.
zz[SYS] Role - BrightStor ARCserve Server	Zeigt alle BrightStor ARCServe-Server an.
zz[SYS] Role - Citrix Server	Zeigt alle Citrix-Server an.
zz[SYS] Role - DHCP Server	Zeigt alle MS DHCP-Server an.
zz[SYS] Role - DNS Server	Zeigt alle MS DNS-Server an.
zz[SYS] Role - Domain Controller	Zeigt alle MS AD Domain Controller-Server an.
zz[SYS] Role - Exchange 2003 Server	Zeigt alle MS Exchange 2003-Server an.
zz[SYS] Role - Exchange 2007 Server	Zeigt alle MS Exchange 2007-Server an.
zz[SYS] Role - Exchange 2010 Server	Zeigt alle MS Exchange 2010-Server an.
zz[SYS] Role - Exchange Server	Zeigt alle MS Exchange-Server an.
zz[SYS] Role - File Server	Zeigt alle MS Dateiserver mit Dateifreigabe(n) durch Nichtadministratoren an.
zz[SYS] Role - FTP Server	Zeigt alle MS FTP-Server an.
zz[SYS] Role - IIS Server	Zeigt alle MS IIS-Server an.
zz[SYS] Role - IMAP4 Server	Zeigt alle MS IMAP4-Server an.
zz[SYS] Role - POP3 Server	Zeigt alle MS POP3-Server an.
zz[SYS] Role - Print Server	Zeigt alle MS Druckerserver mit Dateifreigabe(n) durch Nichtadministratoren an.
zz[SYS] Role - SharePoint Server	Zeigt alle MS SharePoint-Server an.
zz[SYS] Role - SMTP Server	Zeigt alle MS SMTP-Server an, die nicht zugleich auch MS Exchange-Server sind.
zz[SYS] Role - SQL Server	Zeigt alle MS SQL Server an.
zz[SYS] Role - SQL Server (Default Instance)	Zeigt alle MS SQL-Server an, die mit der Standardinstanz eingerichtet sind.
zz[SYS] Role - SQL Server 2005	Zeigt alle MS SQL 2005-Server an.
zz[SYS] Role - SQL Server 2008	Zeigt alle MS SQL 2008-Server an.
zz[SYS] Role - Terminal Server	Zeigt alle MS Terminal-Server im Anwendungsmodus an.
zz[SYS] Role - WINS Server	Zeigt alle MS WINS-Server an.

Patch/Update-Management

Ziel

Das Ziel besteht darin, eine Routinestrategie für das Patch/Update-Management verwalteter Rechner bereitzustellen, die das Scannen und Patchen, Patch-Bestätigungsrichtlinien, die Steuerung des Patchverhaltens, die Transparenz des Patch-Status/der Compliance zur Unterstützung der Entscheidungsfindung sowie die Fehlerbehebung umfasst.

Überblick

Das Patch-Management von Kaseya unterstützt ausschließlich Microsoft Windows-Patches. Der

Patch-Status eines Rechners wird durch einen Patch-Scan ermittelt, und die Patch-Implementierung erfolgt im Rahmen eines automatischen Updates, einer Anfangsaktualisierung, eines Rechner-Updates oder einer Patch-Aktualisierung. Im Rahmen eines Patch-Scans werden sowohl die auf einem Rechner installierten als auch fehlende Patches ermittelt; dadurch wird es möglich, eine geeignete Patchingstrategie festzulegen. Die im Rahmen eines Patch-Scans ermittelten Patches werden in einer Auflistung von Patch-Richtlinien dargestellt, anhand derer anschließend kontrolliert werden kann, welche Patches zur Bereitstellung auf den Rechnern zugelassen werden. Im Rahmen eines automatischen Updates werden zugelassene Patches nach Plan und auf der Grundlage der Zugehörigkeit der jeweiligen Rechner zu den Patch-Richtlinien auf den Rechnern bereitgestellt. Im Rahmen von Anfangsaktualisierungen, Rechner-Updates und Patch-Aktualisierungen stehen Funktionen zur Planung einmaliger oder manueller Aktualisierungen für die allgemeine Patchingstrategie zur Verfügung. Um die Informationen zum Patch-Status stets aktuell zu halten, damit auf deren Grundlage fundierte Entscheidungen bezüglich der Bereitstellung und Zulassung von Patches getroffen werden können, ist es wichtig, dass die Patch-Scans in regelmäßigen Abständen durchgeführt werden. Da auch die regelmäßige Bereitstellung von Patches für eine erfolgreiche Patch-Verwaltung unabdingbar ist, ist es wichtig, automatische Updates zu terminieren. Mithilfe der Patch-Verwaltung können diese wiederkehrenden Aufgaben geplant werden. Die Patch-Verwaltungs umfasst auch einen Satz an Patch-Richtlinien, denen verschiedene Rechner entweder automatisch oder manuell zugewiesen werden können. Bei dieser Strategie der Patch-Verwaltung müssen einfache Wege zum Lokalisieren spezifischer Systeme anhand von Details installierter und/oder fehlender Patches, der Menge fehlender Patches und Rechner in bestimmten Patch-Richtlinien existieren, und es muss bei Bedarf eine Möglichkeit zur Berichterstattung und zum effizienten Handeln in Bezug auf diese Rechnergruppe existieren. Zusätzlicher Inhalt, der im Lieferumfang dieses Pakets enthalten ist, bietet grundlegenden Support für Macintosh Software-Aktualisierungen und Linux Package Aktualisierungen/Upgrades.

Richtlinien

Es werden Richtlinien bereitgestellt, die wiederkehrende Patch-Scan- und automatische Update-Zeitpläne auf die Windows-Rechner anwenden, die innerhalb der verfügbaren IT-Infrastruktur unterstützt werden. Diese Richtlinien aktivieren die wiederkehrende Erkennung installierter und fehlender Patches bei allen Rechnern sowie die Planung der Implementierung aller bestätigten Patches. Es sind ebenfalls Richtlinien enthalten, um Windows-Servern und Arbeitsplatzrechnern die entsprechenden Patch-Richtlinien zuzuweisen und das Nicht-Patchen bestimmter Rechner oder die Einstellung einer Testgruppe zur Implementierung von Patches vor einer allgemeinen Bestätigung und der Implementierung neuer Patches zu unterstützen. Es wird eine zusätzliche Richtlinie bereitgestellt, die wiederkehrende Macintosh-Softwareaktualisierungs-Zeitpläne auf die Macintosh-Rechner anwendet, die innerhalb der IT-Infrastruktur unterstützt werden.

Die eingeschlossenen Richtlinien befinden sich unter **[System].Core.Org Specific Policies.Patch / Update Management**, und sind im Folgenden beschrieben.

- **Windows.Common Windows Patch Mgmt Settings**
  - **Patch-Einstellungen ablehnen -** Wendet Einstellungen der Patch-Verwaltung auf Rechner an, die in der Ansicht der "zz[SYS] Policy - Patch_Deny Patching Group‘ ausgewählt werden. Legt Neustart-Aktion auf „Nicht neu starten nach Aktualisierung“ fest. Legt Zugehörigkeit zu Patch-Richtlinie auf Patch-Richtlinie „Patching ablehnen“ fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen‘ generiert wird, wenn eine „Patch-Installation fehlschlägt“ oder die „Agent-Anmeldedaten ungültig sind oder fehlen“.
  - **Patch-Einstellungen prüfen -** Wendet Einstellungen der Patch-Verwaltung auf Rechner an, die in der Ansicht der "zz[SYS] Policy - Patch_Test Patching Group‘ angewendet werden. Legt Neustart-Aktion fest auf „Falls der Benutzer angemeldet, Neustart anfragen alle 60 Minuten bis zum Neustart. Neustart, wenn der Benutzer nicht angemeldet ist“. Legt Zugehörigkeit zu Patch-Richtlinie auf Patch-Richtlinie „Patchen testen“ fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen‘ generiert wird, wenn eine „Patch-Installation fehlschlägt“ oder die „Agent-Anmeldedaten ungültig sind oder fehlen“.

- **Automatische Windows-Aktualisierung deaktivieren** – Deaktiviert die automatische Windows-Aktualisierung auf Rechnern, auf denen die automatische Aktualisierung durch Windows Update aktiviert ist. Wenn die automatische Aktualisierung durch Windows Update aktiviert ist und Patch-Management von Kaseya verwendet wird, kann das automatische Update von Windows mit der Strategie zum Patch-Management von Kaseya in Konflikt geraten und zur Implementierung von Patches führen, die abgelehnt wurden oder für die in Kaseya immer noch eine Bestätigung aussteht.
- **Dateiquelle Internet** - Stellt die Dateiquelle für Patch-Verwaltung für alle Windows-Rechner auf „Internet", sodass Patches direkt von den Microsoft Patch- und Downloadservern heruntergeladen werden. Diese Richtlinie ist die Standardeinstellung und kann durch eine andere Richtlinie überschrieben werden, die für bestimmte Organisationen oder Rechnergruppen gilt und die Vorrang vor dieser Richtlinie hat.

- **Windows.Windows Workstation Patch Mgmt Settings**
  - **Workstation-Patch-Einstellungen** - Wendet Einstellungen der Patch-Verwaltung auf Windows-Arbeitplatzrechner an. Legt Neustart-Aktion fest auf „Falls der Benutzer angemeldet, Neustart anfragen alle 60 Minuten bis zum Neustart. Neustart, wenn der Benutzer nicht angemeldet ist". Legt Zugehörigkeit zu Patch-Richtlinie auf Patch-Richtlinie „Patchen von Workstations" fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen' generiert wird, wenn eine „Patch-Installation fehlschlägt" oder die „Agent-Anmeldedaten ungültig sind oder fehlen".
  - **Täglicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mo-Fr 06:00–18:00 Uhr/Energiemanagement)** – Liefert Elementen von Workstation-Patch-Richtlinien, bei denen zehn oder mehr bestätigte Patches fehlen, tägliche Zeitpläne für automatische Updates. Automatische Updates sind für Mo-Fr zwischen 06:00 und 18:00 Uhr geplant. Diese Richtlinie wird in der Regel verwendet, wenn bei den Rechnern des Kunden relativ viele Patches fehlen und der Kunde diese Systeme innerhalb von einigen Tagen anstatt einiger Wochen auf den neuesten Stand bringen möchte. Sobald die Rechner gepatcht sind, müssen sie nicht mehr täglich gepatcht werden. Automatische Updates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, die Energieverwaltungsoption jedoch zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.
  - **Wöchentlicher Wkst.-Zeitplan (Scan Di. 06:00–18:00 Uhr/Autom. Update Mi. 06:00–18:00 Uhr/Energiemanagement)** – Liefert Elementen von Workstation-Patch-Richtlinien wöchentliche Zeitpläne für Patch-Scans und automatische Updates. Patch-Scans sind für dienstags zwischen 06:00 und 18:00 Uhr geplant und automatische Updates für mittwochs zwischen 06:00 und 18:00 Uhr. Diese Richtlinie wird in der Regel verwendet, wenn Kunden einen offensiveren Ansatz beim Patchen verfolgen und möchten, dass neue Patches relativ schnell auf den Rechnern bereitgestellt werden, um das Risiko durch nicht gepatchte Rechner zu senken. Automatische Updates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, die Energieverwaltungsoption jedoch zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.
- **Windows.Windows Server Patch Mgmt Settings**
  - **Server-Patch-Einstellungen** - Wendet Einstellungen der Patch-Verwaltung auf Windows-Servern an. Legt Neustart-Aktion auf „Nicht neu starten nach Aktualisierung" fest, „Wenn Neustart erforderlich, E-Mail an E-Mail-Adresse zur Patch-Benachrichtigung senden." Legt Zugehörigkeit zu Patch-Richtlinie auf Patch-Richtlinie „Patchen von Servern" fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen' generiert wird, wenn eine „Patch-Installation fehlschlägt" oder die „Agent-Anmeldedaten ungültig sind oder fehlen".
  - **Wöchentlicher Serverzeitplan (Scan Mi. 18:00-06:00 Uhr)** – Liefert Elementen der Server-Patch-Richtlinie einen Patch-Scan-Zeitplan. Patch-Scans sind für mittwochs

zwischen 18:00 und 06:00 Uhr geplant. Bei dieser Richtlinie sind keine Implementierungen von automatischen Updates auf Servern geplant.

- **Macintosh.Macintosh Workstation Software Update Settings**
  - **Wöchentliches Softwareupdate von Macintosh-Workstation (Installation für mittwochs 18:00-06:00 Uhr empfohlen)** – Führt jede Woche mittwochs ein Mac-Softwareupdate aus, bei dem empfohlene Macintosh-Softwareupdates auf Macintosh-Workstations installiert werden. Softwareupdates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, deren Energieverwaltungsoption jedoch zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

Richtlinien zur Patch-Bestätigung/-Ablehnung

> **Hinweis:** Bei ''Richtlinien'' zur Patch-Bestätigung/-Ablehnung handelt es sich um einen spezialisierten Richtlinientyp im Modul der Patch-Verwaltung, die nicht mit Richtlinien verwechselt werden dürfen, die bei der Verwendung des **Policy Management**-Moduls festgelegt werden. **Policy Management**Es wurden Richtlinien erstellt, die vordefinierte Richtlinien zur Patch-Bestätigung/-Ablehnung spezifizieren.

Es wird ein Satz vordefinierter Patch-Richtlinien zur Verfügung gestellt, um Bestätigung und Ablehnung unterschiedlicher Windows-Patches zu steuern, die auf die unterstützte Windows-Software sowie Windows-Betriebssysteme anwendbar sind.

Name der Patch-Regel	Beschreibung
zz[SYS] Deny Patching	Wird zum Ablehnen aller Patches in Fällen verwendet, in denen Rechner nicht aus einem bestimmten Grund gepatcht werden müssen. Der Standard-Bestätigungsstatus für neue Patches aller Microsoft-Sicherheitsklassifikationen ist auf „Abgelehnt" eingestellt. Siehe Verwalten von Richtlinien-Zugehörigkeit für weitere Informationen darüber, wie Rechner dieser Patch-Richtlinie zugewiesen werden können.
zz[SYS] Server Patching	Wird zum Bestätigen und Ablehnen von Patches für Windows-Server verwendet. Der Standard-Bestätigungsstatus für neue Patches aller Microsoft-Sicherheitsklassifikationen ist auf „Bestätigung ausstehend" eingestellt. Alle Windows-Server werden Teil dieser Patch-Richtlinie, wenn die Patch-Verwaltung des Servers über das automatisierte System-Management aktiviert wird.
zz[SYS] Test Patching	Wird zum Bestätigen und Ablehnen von Patches für Rechner verwendet, die zum Testen von Patches vor der allgemeinen Implementierung auf Windows-Servern und Arbeitsplatzrechnern verwendet werden. Der Standard-Bestätigungsstatus für neue Sicherheit mit hoher Priorität und kritischen Updates, basierend auf deren Microsoft-Sicherheitsklassifizierung, ist auf „Bestätigt" eingestellt. Alle Windows-Server werden Teil dieser Patch-Richtlinie, wenn die Patch-Verwaltung des Servers über das automatisierte System-Management aktiviert wird. Siehe Verwalten von Richtlinien-Zugehörigkeit für weitere Informationen darüber, wie Rechner dieser Patch-Richtlinie zugewiesen werden können.
zz[SYS] Workstation Patching	Wird zum Bestätigen und Ablehnen von Patches für Windows-Arbeitsplatzrechner verwendet. Der Standard-Bestätigungsstatus für neue Sicherheit mit hoher Priorität und kritischen Updates, basierend auf deren Microsoft-Sicherheitsklassifizierung, ist auf „Bestätigt" eingestellt. Alle Windows-Arbeitplatzrechner werden Teil dieser Patch-Richtlinie, wenn die Patch-Verwaltung des Arbeitplatzrechners über das automatisierte System-Management aktiviert wird.

Ansichten

Ein Reihe von vordefinierten Ansichten wird zur Verfügung gestellt, die für die Verwaltung von IT-Diensten und für die Unterstützung des Dienstes zum Patch/Update-Management verwendet werden können. In diesen Ansichten können Sie Maschinen im gesamten System anhand ihrer Patch-Konfiguration, der Menge fehlender Patches, des Patch-Neustart-Status, der Zugehörigkeit zu Patch-Richtlinie usw. zu filtern. Die folgenden Ansichten können sowohl für Reportingzwecke als auch für betriebliche Aktivitäten genutzt werden.

Ansichtsname	Beschreibung
zz[SYS] Patch - Deny Patching Policy	Zeigt alle zugewiesenen Rechner als Mitglieder der Patch-Richtlinie "zz[SYS] - Deny Patching".
zz[SYS] Patch - Missing 10+ Approved Patches	Zeigt alle Rechner an, bei denen 10 oder mehr bestätigte Patches, basierend auf den Richtlinien-Zugehörigkeiten der Rechner-Patches und den bestätigen Patches innerhalb dieser Richtlinien, fehlen.
zz[SYS] Patch - Missing 20+ Approved Patches	Zeigt alle Rechner an, bei denen 20 oder mehr bestätigte Patches, basierend auf den Richtlinien-Zugehörigkeiten der Rechner-Patches und den bestätigen Patches innerhalb dieser Richtlinien, fehlen.
zz[SYS] Patch - No Policy	Zeigt alle Rechner an, die keiner Patch-Richtlinie zugewiesen sind
zz[SYS] Patch - Pending Reboot	Zeigt alle Rechner mit einer ausstehenden Patch-Bereitstellung an, die mit einem Neustart in Verbindung steht.
zz[SYS] Patch - Scan Failed	Zeigt alle Rechner an, bei denen aus irgendeinem Grund der letzte Patch-Scan fehlgeschlagen ist.
zz[SYS] Patch - Scan Not Scheduled	Zeigt alle Rechner an, denen kein Patch-Scan zugewiesen ist.
zz[SYS] Patch - Server Patching Policy	Zeigt alle Rechner an, die ein Mitglied der Patch-Richtlinie "zz[SYS] - Server Patching" sind
zz[SYS] Patch - Servers w No Policy	Zeigt alle Server-Rechner an, die keiner Patch-Richtlinie zugewiesen sind
zz[SYS] Patch - Test Patching Policy	Zeigt alle Rechner an, die ein Mitglied der Patch-Richtlinie "zz[SYS] Test Patching" sind.
zz[SYS] Patch - Windows Auto Update Enabled	Zeigt alle Rechner an, bei denen das automatische Windows-Update aktiviert ist, basierend auf den Erkenntnissen während des letzten Patch-Scans.
zz[SYS] Patch - Workstation Patching Policy	Zeigt alle Rechner an, die ein Mitglied der Patch-Richtlinie "zz[SYS] - Workstation Patching" sind
zz[SYS] Patch - Workstations w No Policy	Zeigt alle Arbeitplatzrechner an, die keiner Patch-Richtlinie zugewiesen sind

Skripting

Es steht Skripting zur Verfügung, das benutzerdefinierte Automatisierungen zur Unterstützung des IT-Dienstes für das Patch/Update-Management durchführt. Dieses Skripting befindet sich unter dem **System**-Cabinet der Seite Skripting > **Planen/Erstellen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2845.htm)*.

- **Systemwiederherstellungspunkt der Patch-Verwaltung erstellen** - Läuft als Vorverfahren für automatische Updates. Wiederherstellungspunkte können während einer Wiederherstellung verwendet werden, falls ein installiertes Patch/Update Probleme bereitet.
  - **Ort:** System.Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore.Create Patch Management System Restore Point

- **Beschreibung:** Verwendet WMIC, um einen Systemwiederherstellungspunkt mit dem Namen "Patch-Verwaltung" zu erstellen. Dieses Skripting kann vor einer Patch-Bereitstellung durch eine Pre-Agent-Prozedur für automatische Updates aufgerufen werden.
- **Ausgeführt von Richtlinie:** System.Core.Org Specific Policies.Patch/Update Management.Windows Workstation Patch Settings.Workstation Patch Settings

- **Mac-Softwareaktualisierung – Empfohlene Aktualisierungen installieren und Ergebnisse abrufen/protokollieren**
  - **Ort:** System.Core.2 Macintosh Procedures.Software Update.Mac Software Update - Empfohlenen Aktualisierungen installieren und Ergebnisse abrufen/protokollieren
  - **Beschreibung:** Installiert empfohlene Mac-Softwareaktualisierungen.
  - **Ausgeführt von Richtlinie:** System.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings.Monthly Softwareupdate von Macintosh-Workstation (Installation für 1. Mi. 18:00-06:00 Uhr empfohlen)

Routinewartung

Ziel

Eine Strategie zur Routinewartung für verwaltete Maschinen zur Verfügung stellen, um Systemoptimierung sowie vorbeugende Wartungsvorgänge wie Diskreinigung und Löschen von temporären Dateien, Festplattenanalyse, -reparatur, -optimierung u. a. einzuschließen. Routinewartungen sind wichtig, um einen gleichmäßigen Betrieb der Systeme bei Spitzenwerten zu gewährleisten. Einen grundlegenden automatisierten Routinewartungsplan für alle unterstützten Systeme einführen, der zunächst für Arbeitsplatzrechner gilt, jedoch erweiterbar und bei Bedarf zur Unterstützung erweiterter Wartungsvorgänge über Zeit sowie von Servern fähig ist.

Überblick

Kaseya Automation, genannt Skripting, kann verwendet werden, um automatisierte Aufgaben in einem oder mehreren Systemen auf einer geplanten Basis durchzuführen. Automatische Aufgaben wie Check Disks, Disk-Fragmentierungsanalyse und -optimierung, Volumenreparatur, Gehäusereinigung, Löschen von Speichern, Bereinigung von temporären Dateien, Protokoll-Rotation u. a. werden in einer leistungsstarken Routinewartungs-Lösung kombiniert, die auf Windows- und Macintosh-Arbeitsplatzrechner angewendet wird, um einen gleichmäßigen Betrieb dieser Systeme zu gewährleisten.

Richtlinien

Ein Satz von Richtlinien gilt für wiederkehrende Routinewartungs-Zeitpläne bei allen Windows- und Macintosh-Arbeitsplatzrechnern. Diese Richtlinien verursachen wiederum Skripting, das die tatsächliche Wartung auf allen Systemen und zu regelmäßigen geplanten Zeiten durchführt. Die eingeschlossenen Richtlinien befinden sich unter **[System].Core.Org Specific Policies.Routine Maintenance**, und sind im Folgenden beschrieben.

- **Wiederkehrende Wartung der Windows-Arbeitplatzrechner**
  - **Windows Workstation-Wartung (Wöchentlich Mo-Fr 18:00-06:00 Uhr)** - Wendet ein geplantes Windows Workstation-Wartungsverfahren auf alle Windows-Arbeitplatzrechnern wöchentlich (Mo-Fr) zwischen 18:00-06:00 Uhr an. Wenn die Maschine zu dem Zeitpunkt nicht eingeschaltet ist, zu dem die Wartung geplant ist, überspringt die Maschine den Wartungszyklus und versucht, die Wartung eine Woche später durchzuführen.
- **Wiederkehrende Wartung der Macintosh Arbeitplatzrechner**
  - **Macintosh Workstation-Wartungsplan (Wöchentlich Mo-Fr 18:00-06:00 Uhr)** - Wendet ein geplantes Macintosh Wartungsverfahren auf alle Macintosh Arbeitplatzrechnern wöchentlich (Mo-Fr) zwischen 18:00-06:00 Uhr an. Wenn die Maschine zu dem Zeitpunkt nicht eingeschaltet ist,

zu dem die Wartung geplant ist, überspringt die Maschine den Wartungszyklus und versucht, die Wartung eine Woche später durchzuführen.

Skripting

Skriptings führen unterschiedliche Aspekte der Wartungsaufgaben auf Windows- und Macintosh-Arbeitsplatzrechnern durch. Diese Verfahren werden gemäß den Richtlinien geplant, um in einem wiederkehrenden Plan ausgeführt zu werden. Die eingeschlossenen Skriptings befinden sich unter **[System].Core**, und sind im Folgenden beschrieben.

- **1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance.Workstation Weekly Maintenance**
  - **Beschreibung:** Führt alle wöchentlichen Desktop-Wartungsaufgaben durch, plant das Ausführen des Skripts während des Wartungsfensters.
  - **Nutzung:** Gemäß Richtlinien-Verwaltung dafür vorgesehen, auf allen Windows-Arbeitplatzrechnern wöchentlich (Mo-Fr) zwischen 18:00 und 06:00 Uhr über die Richtlinie ‚Windows-Arbeitplatzrechnerwartung (Wöchentlich Mo-Fr 18:00-06:00 Uhr)' ausgeführt zu werden, wenn die Funktion Workstation-Wartung über automatisiertes System-Management aktiviert ist.
- **Common Maintenance Tasks.System Restore.Create Weekly Desktop Maintenance System Restore Point**
  - **Beschreibung:** Verwendet WMIC, um einen Systemwiederherstellungspunkt mit dem Namen "Wöchentliche Desktop-Wartung" zu erstellen. Dieses Skripting kann zu Beginn des wöchentlichen Wartungsverfahrens des Arbeitplatzrechners aufgerufen werden.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.
- **Common Maintenance Tasks.Flush DNS. DNS-Resolver-Cache leeren**
  - **Beschreibung:** Leert die Inhalte des DNS-Client-Resolver-Cache und setzt diese zurück, indem IPCONFIG /FLUSHDNS ausgeführt wird
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.
- **Common Maintenance Tasks.IE Files Management. Temporäre Internet Explorer-Dateien löschen**
  - **Beschreibung:** Löscht die temporären Dateien des Internet Explorer für den gegenwärtig angemeldeten Benutzer.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.
- **Common Maintenance Tasks.TEMP Files.TEMP-Ordner des Benutzers löschen.**
  - **Beschreibung:** Löscht alle Dateien und Ordner innerhalb und unterhalb des %TEMP%-Ordners des angemeldeten Benutzers, die nicht aktuell durch Windows gesperrt/geöffnet sind.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.
- **Common Maintenance Tasks.Disk Cleanup.Windows Disk Cleanup**
  - **Beschreibung:** Legt die "sageset"-Registrierungseinträge für cleanmgr.exe fest und führt dann die Datei cleanmgr.exe mit dem Parameter "sagerun" aus, um Dateien an den folgenden Speicherorten automatisch zu bereinigen: Aktiver Setup Temporärer Ordner Inhaltsindizierung Bereiniger Heruntergeladene Programmdateien Internet-Cache-Dateien Speicherauszug Alte ChkDsk-Dateien Papierkorb Remote-Desktop-Cache-Dateien Setup-Protokolldateien Temporäre Dateien Temporäre Offline-Dateien WebClient und WebPublisher Cache
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.
- **Common Maintenance Tasks.Check Disk.Disk prüfen Systemlaufwerk (Planen beim nächsten Neustart)**
  - **Beschreibung:** Führt einen CHKDSK-Befehl im Systemlaufwerk aus. Die Ergebnisse der Wartung werden durch das Skript "Disk Verify prüfen" bewertet.

  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.

- **Common Maintenance Tasks.Defragmentation.Defragment System Drive (Analyse & Benutzer auffordern, wenn erforderlich)**
  - **Beschreibung:** Führt eine Defragmentationsanalyse im Systemlaufwerk in Windows durch (üblicherweise C:). Defragmentationsergebnisse werden in dem Skripting-Protokoll gespeichert. Wenn ein Benutzer am Rechner angemeldet ist, wird er vom Verfahren gefragt, ob eine vollständige Defragmentierung des Laufwerks durchgeführt werden soll und führt diese aus, wenn der Benutzer mit Ja antwortet.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Wartung des Arbeitplatzrechners.
- **2 Macintosh Procedures.Maintenance.Macintosh Weekly Maintenance**
  - **Beschreibung:** Führt eine Reihe von Routine-Wartungsaufgaben auf einem Macintosh OS X-Rechner aus.
  - **Nutzung:** Gemäß Richtlinien-Verwaltung dafür vorgesehen, auf allen Macintosh-Arbeitplatzrechnern wöchentlich (Mo-Fr) zwischen 18:00-06:00 Uhr über die Richtlinie, Planung der Macintosh Arbeitplatzrechnerwartung (Wöchentlich Mo-Fr 18:00-06:00 Uhr)‘ ausgeführt zu werden, wenn die Funktion Workstation-Wartung über automatisiertes System-Management aktiviert ist.
- **Allgemeine Reinigung OS X**
  - **Beschreibung:** Führt Systemreinigung durch, entfernt alte Protokolldateien, Arbeits- und Junk-Dateien, löscht Benutzer- und Systemcaches, rotiert System- und Anwendungsprotokolle, erstellt DYLD-Cache und Spotlight-Index neu.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Macintosh Wartung.
- **OS X Disk-Volumes prüfen und reparieren**
  - **Beschreibung:** Führt Diskprüfung und Reparaturen mithilfe von DISKUTIL durch.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Macintosh Wartung.
- **OS X Disk-Berechtigungen reparieren**
  - **Beschreibung:** Führt eine Disk-Reparatur und einen Berechtigungsvorgang mithilfe von DISKUTIL aus.
  - **Nutzung:** Aufgerufen durch das Verfahren zur wöchentlichen Macintosh Wartung.

Monitoring

In diesem Abschnitt

Übersicht über die Monitoring-Merkmale

Ziel

Eine Strategie für das Monitoring zur Überwachung und Benachrichtigung über Hardware- und Software-Bestände zur Verfügung stellen. Monitoring kritischer Systemereignisse auf Windows-Servern rund um die Uhr, sieben Tage die Woche, stellt die Funktionsfähigkeit Ihrer IT-Infrastruktur sicher. Falls ein Problem auftreten sollte, kann es bei ausbleibender sofortiger Benachrichtigung zur materiellen Beeinträchtigung der Business Continuity kommen. Da sich die Rechner innerhalb der IT-seitig unterstützten Infrastruktur im Laufe der Zeit verändern, wird ein entsprechendes Monitoring eingesetzt, um diese Veränderungen zu erkennen und das Monitoring entsprechend auf diese Veränderungen abzustimmen.

Überblick

Mit Kaseya-Monitoring sind unterschiedliche Monitoring-Vorgehensweisen für Agent-basierte und nicht-Agent-basierte Systeme innerhalb einer kundenseitigen IT-Infrastruktur möglich. Das Monitoring der Server-Verfügbarkeit in Form von "Agentstatus-Benachrichtigungen" ermöglicht Benachrichtigungen, sobald das System aufgrund von Abstürzen, Neustarts, Netzwerkkonnektivität, Systemüberlastung usw. herunterfährt oder anderweitig ‚offline' ist. Das Monitoring des Windows-Dienstes in Form von Monitor-Sets mit Dienstprüfungen bietet ein regelmäßiges Monitoring wichtiger Windows-Dienste, sendet Benachrichtigungen und führt eine automatische Sanierung (Neustartdienste) durch, wenn diese Dienste nicht funktionieren bzw. gestoppt sind. Das Monitoring des Ereignisprotokolls in Form von Ereignis-Satz-Benachrichtigungen bietet ein durchgehendes Monitoring der Windows-Ereignisprotokolle und sendet Benachrichtigungen, wenn wichtige Ereignisse in diesen Windows-Ereignisprotokollen protokolliert werden. Das Leistungs-Monitoring in Form von Monitor-Sets mit Zähler-Schwellenwerten bietet ein durchgehendes Monitoring wichtiger Windows-Leistungsindikatoren und sendet Benachrichtigungen, sobald die Werte des Zählers bestimmte Schwellenwerte erreichen, was einen negativen Einfluss auf die Systemleistung, Verfügbarkeit und/oder Zuverlässigkeit haben kann. Monitoring-Status, Ereignisse und Werte für Zähler werden innerhalb des Systems protokolliert, um Verlaufs-, Trend- sowie Berichtsinformationen zu aktualisieren. Alarme, die durch Überwachungssysteme erzeugt werden, werden innerhalb des Systems protokolliert (zur Verlaufs- und Berichterstellung). Mehrere Schweregrade werden unterstützt, sodass Probleme, die nicht auftreten, entsprechend priorisiert werden können und die richtigen Personen per E-Mail benachrichtigt werden können.

Der folgende Überblick über die Monitoring-Merkmale stellt das im Standardlösungspaket enthaltene System und die Monitoring-Typen dar.

Monitoring-Typen = (A=Verfügbarkeit, E=Ereignisprotokoll, S=Services, P=Leistung)

Systemtyp (Kategorie)	Monitortypen	Allgemeine Übersicht über das Monitoring
Alle Windows Server (OS)	AESP	Core Win Srvr Monitoring
Windows Server 2003 (Betriebssystem)	--S-	Win 2003 Dienste
Windows Server 2008/2008 R2 (Betriebssystem)	--S-	Win 2008/2008R2 Dienste

Durch den Setup-Assistenten aktivierte Inhalte

Alle Windows-Arbeitplatzrechner (Betriebssystem)	AESP	Core Win Wkst Monitoring
Windows Vista (Betriebssystem)	--S-	Win Vista Dienste
Windows 7 (Betriebssystem)	--S-	Win 7 Dienste
Windows XP (Betriebssystem)	--S-	Win XP Dienste
Dell PowerEdge (Hardware)	-E--	Dell PowerEdge HW-Ereignisse
HP ProLiant (Hardware)	-E--	HP ProLiant HW Ereignisse
IBM Serie x (Server-Hardware)	-E--	IBM Series x HW-Ereignisse
Backup-Exec-Server (Rolle)	-ES-	Backup Exec Monitoring
Blackberry Enterprise Server	-ESP	Blackberry-Server-Monitoring
BrightStor ARCServe Server	-ES-	BrightStor Server Monitoring
Citrix-Server	-ES-	Citrix-Server-Monitoring
DHCP-Server	-ESP	DHCP-Server-Monitoring
DNS-Server	-ESP	DNS-Server-Monitoring
Domain-Controller (Netzwerk Infra)	-ESP	DC/Active Directory Monitoring
Exchange 2003 Server (E-Mail)	-ES-	Exch 2003 Monitoring
Exchange 2007 Server (E-Mail)	-ES-	Exch 2007 Monitoring
Exchange 2010 Server (E-Mail)	-ESP	Exch 2010 Monitoring
Exchange Server (E-Mail)	-ESP	Core Exchange Monitoring
Dateiserver (Datei/Drucken)	--S-	Dateiserver-Monitoring
FTP-Server (Websysteme)	--S-	FTP-Server-Monitoring
IIS Server (Websysteme)	-ESP	IIS-Server-Monitoring
IMAP4-Server (E-Mail)	--S-	IMAP4 Server-Monitoring
POP3-Server (E-Mail)	--S-	POP3 Server-Monitoring
Druckerserver (Datei/Drucken)	-ESP	Druckerserver-Monitoring
Microsoft SE-FEP (Sicherheit)	-ES-	Microsoft SE-FEP Monitoring
SharePoint Server (Websysteme)	--S-	SharePoint Server-Monitoring
SMTP-Server (E-Mail)	-ESP	SMTP-Server Monitoring
SQL-Server (Datenbank)	--SP	Core SQL Server-Monitoring
SQL Server 2005 (Datenbank)	--S-	SQL Server 2005 Monitoring
SQL Server 2008 (Datenbank)	--S-	SQL Server 2008 Monitoring
Terminal-Server (Remotezugriff)	-ESP	Terminal-Server Monitoring
WINS-Server (Netzwerk-Infra)	--S-	WINS-Server Monitoring
AVG Tech (Sicherheit)	--S-	AVG Tech AV Monitoring
Kaspersky ES (Sicherheit)	--S-	Kaspersky ES Monitoring
McAfee (Sicherheit)	-ES-	McAfee Monitoring
Sophos (Sicherheit)	-ES-	Sophos Monitoring
Symantec AV (Sicherheit)	-ES-	Symantec AV Monitoring
Symantec EP (Sicherheit)	-ES-	McAfee AV Monitoring
Trend Micro (Sicherheit)	-ES-	McAfee AV Monitoring

Monitoring Schweregrad-Matrix

		Monitoring-Aktionen

Schweregrad-Stufe	**Beschreibung**	**E-Mail**	**Alarm**	**Wiederherstellen**
Schweregrad0	Zur Information/Protokollierung	Nein	Nein	Nicht zutreffend
Schweregrad1	Geringer Einfluss/Risiko	Ja	Ja	7 Tage
Schweregrad2	Mittlerer Einfluss/	Ja	Ja	1 Tag
Schweregrad3	Hoher Einfluss/Risiko	Ja	Ja	12 Std
Festgelegte Benachrichtigung	Hoher Einfluss/Risiko	Ja	Ja	12 Std

Hinweis: Schweregrad-Stufen treffen nur auf Monitor-Sets und Ereignis-Sets zu und sind im Namen des Sets gekennzeichnet. Festgelegte Benachrichtigungen sind so konfiguriert, dass sie sich wie Schweregrad3 verhalten.

Monitoring-Richtlinien

Eine Reihe von Richtlinien wendet spezifische *Monitoring*-Konfigurationen auf Rechner an, wobei deren Version und Hardware des Windows-Betriebssystems, die funktionale Rolle sowie Sicherheits-/AntiVirus-Produkte zugrunde gelegt werden. Diese Richtlinien aktivieren die unterschiedlichen Monitoring-Komponenten für Verfügbarkeit, Ereignisprotokolle, Dienste und Leistung sowie die damit verbundene Monitoring-Automatisierung. Die eingeschlossenen Richtlinien befinden sich unter **[System].Core.Org Specific Policies.Monitoring**, und sind im Folgenden beschrieben.

In diesem Abschnitt

Server

- **Allgemeines Windows Server-Monitoring** - Wendet ein allgemeines Monitoring-Set auf alle Windows-Server an. Dies umfasst mit Hardware verknüpfte Ereignisprotokolle, Windows-Dienst und allgemeines Windows-Systemleistungs-Monitoring.
- **Windows-Server (Core)** - Wendet eine Reihe von grundlegenden Windows-Server-Monitoring-Optionen auf Windows-Server an, einschließlich Monitoring für Standard-Dienste, Systemleistung, Integritäts-Reporting, Ereignisprotokolle u. a.
- **Windows-Server 2003** - Wendet Standard-Dienstmonitoring auf Windows 2003 Server an.
- **Windows-Server 2008/2008 R2** - Wendet Standard-Dienstmonitoring auf Windows 2008/2008 R2 Server an.

Hardware

- **Dell PowerEdge** - Wendet hardware-spezifisches Monitoring und Benachrichtigen für Dell PowerEdge Server an. Für dieses Monitoring müssen möglicherweise spezifische Dell PowerEdge Serververwaltungs-Werkzeuge auf dem Serverrechner installiert werden.
- **HP ProLiant** - Wendet hardware-spezifisches Monitoring und Benachrichtigen für HP ProLiant Server an. Für dieses Monitoring müssen möglicherweise spezifische HP ProLiant Serververwaltungs-Werkzeuge auf dem Serverrechner installiert werden.
- **IBM Serie x** - Wendet hardware spezifisches Monitoring und Benachrichtigen für IBM Serie x an. Für dieses Monitoring müssen möglicherweise spezifische IBM Serie X Serververwaltungs-Werkzeuge auf dem Serverrechner installiert werden.

Rollen

- **Backup Exec Server** - Wendet Monitoring auf Backup Exec Server an.
- **Blackberry Enterprise Server** - Wendet Monitoring auf Blackberry Enterprise Server an.
- **BrightStor ARCServe Server** - Wendet Monitoring auf BrightStor Server an.
- **Citrix-Server** – Wendet Monitoring auf Citrix-Server an.
- **DHCP Server** – Wendet Monitoring auf DHCP-Server an.
- **DNS Server** – Wendet Monitoring auf DNS-Server an.
- **Domain-Controller** – Wendet Monitoring auf Domain-Controller an.
- **Exchange 2003 Server** – Wendet Monitoring auf Exchange 2003 Server an.

- **Exchange 2007 Server** – Wendet Monitoring auf Exchange 2007 Server an.
- **Exchange 2010 Server** – Wendet Monitoring auf Exchange 2010 Server an.
- **Exchange Server** – Wendet Monitoring auf Exchange Server an.
- **Dateiserver** - Wendet Monitoring auf Dateiserver an.
- **FTP-Server** - Wendet Monitoring auf FTP-Server an.
- **IIS-Server** - Wendet Monitoring auf IIS-Server an.
- **IMAP4-Server** - Wendet Monitoring auf IMAP4-Server an.
- **POP3-Server** - Wendet Monitoring auf POP3-Server an.
- **Druckerserver** - Wendet Monitoring auf Printserver an.
- **SharePoint Server** - Wendet Monitoring auf SharePoint Server an.
- **SMTP-Server** - Wendet Monitoring auf SMTP-Server an.
- **SQL-Server** - Wendet Monitoring auf SQL-Server an.
- **SQL-Server 2005** - Wendet Monitoring auf SQL 2005 Server an.
- **SQL-Server 2008** - Wendet Monitoring auf SQL 2008 Server an.
- **Terminal-Server** - Wendet Monitoring auf Terminal-Server an.
- **WINS-Server** - Wendet Monitoring auf WINS-Server an.

Arbeitplatzrechner

- **Allgemeines Windows-Arbeitplatzrechner-Monitoring** - Wendet ein allgemeines Monitoring-Set auf alle Windows-Arbeitplatzrechner an. Dies umfasst mit Hardware verknüpfte Ereignisprotokolle, Windows-Dienst und allgemeines Windows-Systemleistungs-Monitoring.
- **Windows-Arbeitplatzrechner (Core)** - Wendet eine Reihe grundlegender Monitoring-Optionen für Windows-Arbeitplatzrechner auf Windows-Arbeitplatzrechner an, einschließlich Monitoring für Standard-Dienste, Systemleistung, Integritäts-Reporting u. a.
- **Windows Vista** - Wendet Standard-Dienstmonitoring für Rechner mit Windows Vista an.
- **Windows 7** - Wendet Standard-Dienstmonitoring für Rechner mit Windows 7 an.
- **Windows XP** - Wendet Standard-Dienstmonitoring für Rechner mit Windows XP an.

Security.Antivirus

- **AVG Tech** - Wendet Monitoring für AVG Technologies AntiVirus an.
- **McAfee** - Wendet Monitoring für McAfee AntiVirus an.
- **Microsoft SE-FEP** - Wendet Monitoring für Microsoft Security Essentials und Forefront Endpoint Protection an.
- **Sophos** - Wendet Monitoring für Sophos AntiVirus an.
- **Symantec AV** - Wendet Monitoring für Symantec AntiVirus an.
- **Symantec EP** - Wendet Monitoring für Symantec Endpoint Protection AntiVirus an.
- **Trend Micro** - Wendet Monitoring für Trend Micro AntiVirus an.

Dienstprogramm

- **Listen durch Scan aktualisieren** - Wendet einen geplanten ‚Listen durch Scan aktualisieren'-Vorgang auf alle Windows-Rechner an, um den Leistungsindikator, das Ereignisprotokoll und aktuelle Dienstinformationen für jeden Rechner für präzise Monitoring-Zwecke auf dem neuesten Stand zu halten.
- **Monitoring-Bereinigung** - Als letzte Richtlinie, die Benachrichtigungen und Monitor-Sets enthält, stellt diese Richtlinie effektiv sicher, dass zuvor angewendetes Monitoring (Ereignisprotokoll-Benachrichtigungen und Monitor-Sets, die über andere Richtlinien zugewiesen wurden, die aufgrund von Rollenänderung nicht länger benötigt werden usw.) entfernt wird.

Monitor-Sets

Eine Reihe von Monitor-Sets wird zur Verfügung gestellt und über die mit dem Monitoring in Verbindung stehenden Richtlinien angewendet. Diese Monitor-Sets überwachen die Windows-Dienste und Leistungsindikatoren mithilfe von Dienstprüfungen und Zähler-Schwellenwerten. Die bereitgestellten Monitor-Sets umfassen u.a. die Überwachung von wichtigen Windows-Betriebssystemdienste und Dienste für übliche Microsoft-Systeme wie Active Directory, Exchange, SQL, IIS u. a. Grundlegendes Systemleistungs-Monitoring für Festplattenspeicher, Speichernutzung, CPU-Verwendung sowie erweiterte systemspezifische Leistungsüberwachung sind enthalten. Die eingeschlossenen Monitor-Sets befinden sich unter **[System].Core**, und sind im Folgenden beschrieben.

In diesem Abschnitt

Backup

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - Überwacht Backup Exec Continuous Protection Services auf Backup Exec-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - Überwacht Backup Exec DLO Agent Services auf Backup Exec Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - Backup Exec Services - {Severity3}**
  - Überwacht Backup Exec Services auf Backup Exec-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - Backup Exec System Recovery Service - {Severity3}**
  - Überwacht Backup Exec-Systemwiederherstellungs-Services auf Backup Exec-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - Überwacht BrightStor ARCServe Backup-Services auf BrightStor ARCServe Backup-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Datenbank

- **Database - SQL Server (All Instances) Services - {Severity3}**
  - Überwacht SQL Server Dienste auf SQL-Servern Dienste unter Verwendung des Wildcard MSSQL*-Dienstes. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server (Default Instance) - {Severity0}**
  - Sammelt SQL-Server (Standardinstanz)-Leistungsindikatoren auf SQL-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Database - SQL Server (Default Instance) Performance - {Severity2}**
  - Überwacht SQL-Server (Standardinstanz)-Leistung auf SQL-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Database - SQL Server (Default Instance) Services - {Severity3}**
  - Überwacht SQL-Server (Standardinstanz)-Dienste auf SQL-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2005 Optional Services - {Severity3}**
  - Überwacht SQL Server 2005-Dienste auf SQL Server 2005-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2005 Services - {Severity3}**
  - Überwacht SQL Server 2005-Dienste auf SQL Server 2005-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2008 Optional Services - {Severity3}**
  - Überwacht SQL Server 2008-Dienste auf SQL Server 2008-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2008 Services - {Severity3}**
  - Überwacht SQL Server 2008-Dienste auf SQL Server 2008-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

E-Mail

- **Email - Blackberry Server Performance - {Severity2}**
  - Überwacht die Blackberry Server-Leistung auf Blackberry-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Email - BlackBerry Server Services - {Severity3}**
  - Überwacht Blackberry Server-Dienste auf Blackberry-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2003 Services - {Severity3}**
  - Überwacht Exchange 2003-Dienste auf Exchange 2003-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2007 Services - {Severity3}**

  - Überwacht Exchange 2007-Dienste auf Exchange 2007-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**
  - Sammelt Leistungsindikatoren von Exchange 2010 Edge-Transport-Warteschlangen auf Exchange 2010-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  - Überwacht die Exchange 2010 Edge-Transport-Warteschlangenleistung auf Exchange 2010-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  - Überwacht die Exchange 2010 Edge-Transport-Warteschlangenleistung auf Exchange 2010-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2010 Services - {Severity3}**
  - Überwacht Exchange 2010-Dienste auf Exchange 2010-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange Client Active Logons - {Severity0}**
  - Sammelt Leistungsindikatoren aktiver Exchange Client-Logins auf Exchange-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - Überwacht den Exchange IMAP4-Dienst auf Exchange-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange POP3 Service - {Severity3}**
  - Überwacht den Exchange POP3-Dienst auf Exchange-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - Überwacht die Leistung von Exchange Server auf Exchange-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Email - Exchange Server (Core) Services - {Severity3}**
  - Überwacht die Exchange Server (Core)-Dienste auf Exchange Server (Core)-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - Sammelt Leistungsindikatoren von Exchange-Speichern und -Datenbanken auf Exchange-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Email - SMTP Queue Performance - {Severity3}**
  - Überwacht die SMTP-Warteschlangenleistung auf SMTP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - SMTP Server Service - {Severity3}**
  - Überwacht den SMTP-Serverdienst auf SMTP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Datei/Drucken

- **File / Print - DFS Service - {Severity3}**
  - Überwacht den DFS-Dienst auf DFS-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **File / Print - DFSR Service - {Severity3}**
  - Überwacht den DFSR-Dienst auf DFSR-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **File / Print - NTFRS Service - {Severity3}**
  - Überwacht den NTFRS-Dienst auf NTFRS-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
  - Überwacht die Leistung von Datei- und Druckservern bei Druckerwarteschlangen-Auftragsfehlern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **File / Print - Spooler Service - {Severity3}**
  - Überwacht den Spoolerdienst auf Datei- und Druckservern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Netzwerkinfrastruktur

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**
  - Überwacht Active Directory-Domänencontrollerdienste auf Active Directory-Domänencontrollern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Network Infrastructure - DHCP Server Performance - {Severity2}**
  - Überwacht die DHCP-Serverleistung auf DHCP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Network Infrastructure - DHCP Server Service - {Severity3}**
  - Überwacht den DHCP-Serverdienst auf DHCP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Network Infrastructure - DNS Server Performance - {Severity2}**
  - Überwacht die DNS-Serverleistung auf DNS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Network Infrastructure - DNS Server Service - {Severity3}**
  - Überwacht den DNS-Serverdienst auf DNS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Network Infrastructure - WINS Server Service - {Severity3}**
  - Überwacht den WINS-Serverdienst auf WINS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

OS Platforms.Windows (Core).Disk Space

- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk C von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk D von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk E von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk F von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk G von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk C von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk D von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk E von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk F von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk G von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.

OS Platforms.Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - Sammelt den Dienststatus für alle automatischen Dienste auf Windows-Rechnern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Windows (Core) - CPU and Memory - {Severity0}**

- Sammelt Leistungsindikatoren von CPU und Speicher auf Windows-Rechnern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.

- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - Überwacht den freien Festplattenspeicher auf allen Laufwerken mit weniger als 1 GB Speicher auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - Überwacht den freien Festplattenspeicher auf allen Laufwerken mit weniger als 2 GB Speicher auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - Überwacht den freien Festplattenspeicher unter 750 MB auf jedem Laufwerk auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk C von Windows-Rechnern, wenn jener unter 1 GB liegt. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows (Core) - Free Disk Space on Drive C Below 2GB - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk C von Windows-Rechnern, wenn weniger als 2 GB Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk C von Windows-Rechnern, wenn jener unter 750 MB liegt. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Machine Health - {Severity0}**
  - Sammelt Leistungsindikatoren zur Integrität von Windows-Rechnern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - Überwacht die Prozessor- und Speicherleistung auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  - Überwacht die TCPv4-Verbindungsleistung auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.

OS Platforms Windows Servers

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - Überwacht die Clusterdienste auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  - Überwacht die Leistung der Festplattenzeit und Warteschlangenlänge auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows Server (Core) - Drive C Performance - {Severity1}**

  - Überwacht die Leistung des Laufwerks C auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Server (Core) - General System Performance - {Severity1}**
  - Überwacht die allgemeine Systemleistung auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Server (Core) - Server Reboots - {Severity1}**
  - Überwacht die Server-Neustarts auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Server (Core) - Standard Services - {Severity3}**
  - Überwacht die Standarddienste auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server 2003 - Standard Services - {Severity3}**
  - Überwacht die Standarddienste auf Windows Server 2003-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server 2008/2008 R2 - Standard Services - {Severity3}**
  - Überwacht die Standarddienste auf Windows Server 2008/2008 R2-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

OS Platforms.Windows Workstations

- **Windows 7 - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows 7-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Vista - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows Vista-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows XP - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows XP-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.

Remotezugriff

- **Remote Access - Citrix Licensing Service - {Severity3}**
  - Überwacht den Citrix-Lizenzierungsdienst auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix Licensing WMI Service - {Severity3}**
  - Überwacht den Citrix-Lizenzierungs-WMI-Dienst auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix MetaFrame Services - {Severity3}**

  - ➢ Überwacht Citrix MetaFrame-Dienste auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix Server Services - {Severity3}**
  - ➢ Überwacht Citrix MetaFrame-Dienste auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**
  - ➢ Überwacht den Citrix-Dienst "Virtual Memory Optimization" (Optimierung des virtuellen Speichers) auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Terminal Server Services - {Severity3}**
  - ➢ Überwacht die Terminalserverdienste auf Terminalservern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Terminal Server Session Performance - {Severity2}**
  - ➢ Überwacht die Terminalserver-Sitzungsleistung auf Terminalservern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.

Sicherheit

- **AV - AVG Tech AVG Services - {Severity3}**
  - ➢ Überwacht AVG Tech-Virenschutzdienste auf Rechnern mit AVG Tech-Virenschutz. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Kaspersky Endpoint Security Services {Severity3}**
  - ➢ Überwacht Kaspersky Endpoint Security-Dienste auf Rechnern mit Kaspersky Endpoint Security. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - McAfee Enterprise Services - {Severity3}**
  - ➢ Überwacht McAfee Enterprise-Dienste auf Rechnern mit McAfee Enterprise. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Sophos Antivirus Services - {Severity3}**
  - ➢ Überwacht Sophos Antivirus-Dienste auf Rechnern mit Sophos Antivirus. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Symantec Antivirus Services - {Severity3}**
  - ➢ Überwacht Symantec Antivirus-Dienste auf Rechnern mit Symantec Antivirus. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Symantec Endpoint Protection Services - {Severity3}**
  - ➢ Überwacht Symantec Endpoint Protection-Dienste auf Rechnern mit Symantec Endpoint Protection. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Trend Micro Client Server Security Services - {Severity3}**
  - ➢ Überwacht Trend Micro Client Server Security-Dienste auf Rechnern mit Trend Micro Client Server Security. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

- **AV - Trend Micro OfficeScan Services - {Severity3}**
  - Überwacht Trend Micro OfficeScan-Dienste auf Rechnern mit Trend Micro OfficeScan. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Websysteme

- **Web Systems - FTP Server Service - {Severity3}**
  - Überwacht den FTP-Serverdienst auf FTP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Web Systems - IIS Performance - {Severity3}**
  - Überwacht die IIS-Leistung auf IIS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Web Systems - IIS Server - {Severity0}**
  - Sammelt IIS-Server-Leistungsindikatoren auf IIS-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Web Systems - IIS Server Services - {Severity3}**
  - Überwacht die IIS-Serverdienste auf IIS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Web Systems - SharePoint Server Services - {Severity3}**
  - Überwacht die SharePoint-Serverdienste auf SharePoint-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Ereignis-Sätze

Eine Reihe von Ereignis-Sätzen wird bereitgestellt und über die Monitoring-bezogenen Richtlinien angewandt. Diese Ereignis-Sets überprüfen Windows-Ereignisprotokolle auf spezifische Ereignisse. Die bereitgestellten Ereignis-Sets umfassen u.a. das Monitoring von wichtigen Windows-Betriebssystemereignissen, von üblichen Microsoft-Systemen wie Active Directory, Exchange, SQL, IIS und von Drittanbieter-Anwendungen/-Systemen. Die enthaltenen Ereignis-Sätze sind im Folgenden erläutert und nach Kategorien unterteilt.

In diesem Abschnitt

Sicherheit

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische McAfee Antivirus-Fehler- und Warnereignisse. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Microsoft Security Essentials/Forefront Endpoint Protection. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - Überprüft die Anwendungs- & System-Ereignisprotokolle auf sonstige spezifische Antivirus-Fehler- und Warnereignisse. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - Überprüft die Anwendungs- & System-Ereignisprotokolle auf sonstige spezifische Antivirus-Informationsereignisse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse bezüglich Symantec/Norton AntiVirus. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse bezüglich Symantec/Norton AntiVirus. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse bezüglich Symantec/Norton AntiVirus. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Informationsereignisse bezüglich Symantec/Norton AntiVirus. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.

Backup

- zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in Backup Exec. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit fehlgeschlagenen/stornierten Aufträgen in Backup Exec. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit erfolgreich ausgeführten Aufträgen in Backup Exec. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in BrightStor ARCserve. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in BrightStor ARCserve. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse beim Backup von Microsoft Windows. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf sonstige spezifische Backup-Fehlerereignisse. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}
  - Überprüft das Anwendungs-Ereignisprotokoll auf sonstige Backup-Informationsereignisse. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf sonstige spezifische Backup-Warnereignisse. Alarme werden als "Schweregrad1" eingestuft.

Datenbank

- zz[SYS] Database - SQL Server (E) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.

- **zz[SYS] Database - SQL Server (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Ereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Backup-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Backup-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Backup-Ereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in den SQL Server-Datenbankressourcen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in den SQL Server-Datenbankressourcen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in den SQL Server-Datenbankressourcen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in den SQL Server-Datenbankressourcen. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}**

- Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.

- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Ereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Netzwerkfehler- und Warnereignisse im Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Netzwerkfehler- und Warnereignisse im Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Abfragefehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Abfragefehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Reportingfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**

  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Reportingfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Reportingereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**
  - ➢ Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**
  - ➢ Überprüft das System-Ereignisprotokoll auf bestimmte Informationsereignisse in Zusammenhang mit dem SQL Server-Cluster. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**
  - ➢ Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit SQL/mit dem Dienststeuerungsmanager. Alarme werden als "Schweregrad3" eingestuft.

E-Mail

- **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Warnereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Warnereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Warnereignisse im Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit Exchange 2000 und 2003. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2000 und 2003. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2000 und 2003. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Exchange 2000, 2003 und 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in Exchange 2007. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Clientzugriff in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**

  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Clientzugriff in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.

- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Clientzugriff in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Edge-Transport in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Edge-Transport in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Edge-Transport in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Hub-Transport in Exchange 2007 betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Hub-Transport in Exchange 2007 betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Hub-Transport in Exchange 2007 betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse, die das Postfach in Exchange 2007 betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse, die das Postfach in Exchange 2007 betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse, die das Postfach in Exchange 2007 betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Postfach in Exchange 2007. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**

- Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Transportdiensten in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.

- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Transportdiensten in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Transportdiensten in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Unified Messaging in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Unified Messaging in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Unified Messaging in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange-Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange-Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Informationsereignisse in Zusammenhang mit dem Exchange-Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**

  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Exchange Server 5.5. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange/mit dem Dienststeuerungsmanager. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem SMTP/Dienststeuerungsmanager. Alarme werden als "Schweregrad3" eingestuft.

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Akku. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Akku. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Akku. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Akku. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Controller. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Controller. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Controller. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Controller. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Elektronik. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Elektronik. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Elektronik. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Dell-Elektronik. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.

- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Gehäuse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Gehäuse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Gehäuse. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Gehäuse. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Umgebung. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Umgebung. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Umgebung. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Dell-Umgebung. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Lüfter. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Lüfter. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Lüfter. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Lüfter. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Alarme werden als "Schweregrad3" eingestuft.

- **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Hardwareprotokoll. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Hardwareprotokoll. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Hardware-Protokoll. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Dell-Medien. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Dell-Medien. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Dell-Medien. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit Dell-Medien. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit einem Vorausfall des Dell-Speichers. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit einem Vorausfall des Dell-Speichers. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSA-System. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSA-System. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSA-System. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**

  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-OMSA-System. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSM-System. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSM-System. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der physischen Dell-Festplatte. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der physischen Dell-Festplatte. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der physischen Dell-Festplatte. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der physikalischen Dell-Festplatte. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Energiemanagement. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Energiemanagement. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Energiemanagement. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Energiemanagement. Alarme werden als "Schweregrad0" eingestuft.
- zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Prozessor. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Prozessor. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}

   - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Prozessor. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Dell-Redundanzspiegelung. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Dell-Redundanzspiegelung. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}**
   - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Dell-Redundanzspiegelung. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Temperatur von Dell Geräten. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Temperatur von Dell Geräten. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Temperatur von Dell Geräten. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**
   - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Temperatur von Dell-Geräten. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der virtuellen Dell-Festplatte. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der virtuellen Dell-Festplatte. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}**
   - Überprüft das System-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit der virtuellen Dell-Festplatte. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}**
   - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die HP Top Tools betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}**
   - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den HP/Compaq Insight Manager betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}**

  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem HP/Compaq StorageWorks-Speicher. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische IBM SeriesX-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf sonstige Hardware-Fehlerereignisse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf sonstige Hardware-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit sonstiger Hardware. Alarme werden als "Schweregrad1" eingestuft.

Netzwerkinfrastruktur

- **zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Audit-Ereignisse in Zusammenhang mit Fehlern bei Active Directory-Anmelde-/-Abmelde-/Sperraktivitäten. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit der Active Directory-NTDS-Datenbankdatei. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit der Active Directory-NTDS-Datenbankdatei. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Active Informationsereignisse in Zusammenhang mit Active Directory. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.

- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit dem DHCP-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Warnereignisse, die den DHCP-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehlerereignisse, die den DNS-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit dem DNS-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit dem WINS-Server. Alarme werden als "Schweregrad1" eingestuft.

Remotezugriff

- **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Citrix MetaFrame. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Citrix-Server-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Terminal-Server-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Terminal-Server-Fehlerereignisse. Alarme werden als "Schweregrad3" eingestuft.

Websysteme

- **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit IIS 6. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit IIS 7. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit IIS 7. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse, die den IIS-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Warnereignisse, die den IIS-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.

Betriebssystemplattformen

- zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Windows Server-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Windows Server-Fehlerereignisse. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Windows Server-Ereignisse. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Fehler-Audit-Ereignisse. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Fehler-Audit-Ereignisse. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Warnereignisse. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Warnereignisse. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}
  - Ignoriert das Monitoring von spezifischen allgemeinen Windows Server-Fehler- und Warnereignissen in den Anwendungs- & System-Ereignisprotokollen.
- zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Druck-Spooler des Windows-Servers betreffen. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Dienststeuerungs-Manager des Windows-Servers betreffen. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Dienststeuerungs-Manager des Windows-Servers betreffen. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Informationsereignisse, die den Dienststeuerungs-Manager des Windows-Servers betreffen. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf Warnereignisse, die das Herunterfahren des Windows Server-Systems betreffen. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Fehlerereignisse bezüglich Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}

  - Überprüft das System-Ereignisprotokoll auf allgemeine Fehlerereignisse bezüglich Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf allgemeine Warnereignisse bezüglich Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der erweiterten Version von Windows Server 2008. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der erweiterten Version von Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische erweiterte Fehler- und Warnereignisse, die erweiterte Windows Server 2008-Funktionen betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf spezifische erweiterte Fehler- und Warnereignisse, die erweiterte Windows Server 2008-Funktionen betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische erweiterte Fehler- und Warnereignisse, die erweiterte Windows Server 2008-Funktionen betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der erweiterten Version von Windows Server 2008. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**
  - Überprüft das Sicherheits-Ereignisprotokoll auf Fehler-Audit-Ereignisse im Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**

  - Überprüft das Sicherheits-Ereignisprotokoll auf Fehler-Audit-Ereignisse im Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**
  - Überprüft das Sicherheits-Ereignisprotokoll auf Fehler-Audit-Ereignisse im Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Fehlerereignisse im Zusammenhang mit Windows-Arbeitplatzrechnern. Alarme werden als "Schweregrad1" eingestuft.

Kapitel 4

Vollständiger Katalog aller Inhalte

Die folgenden Themen enthalten eine Zusammenfassung der vollständigen Liste, die mit der VSA bereitgestellt wird.

In diesem Kapitel

Ansichten

Agentstatus

- zz[SYS] Agent - Has Checked In
  - Zeigt alle Rechner an, die sich mindestens einmal angemeldet haben (ausgenommen Vorlagen)
- zz[SYS] Agent - Has Not Checked In
  - Zeigt alle Agents an, die sich nicht angemeldet haben (z.B. KDS-Implementierungsrechner und -vorlagen)
- zz[SYS] Agent - Offline
  - Zeigt alle Agents an, die seit mehr als 1 Minute offline sind.
- zz[SYS] Agent - Offline 30+ Days
  - Zeigt alles Agents an, die seit mehr als 30 Tagen offline sind.
- zz[SYS] Agent - Offline 60+ Days
  - Zeigt alles Agents an, die seit mehr als 60 Tagen offline sind.
- zz[SYS] Agent - Online
  - Zeigt alle Agents an, die innerhalb der letzten Minute online waren.
- zz[SYS] Agent - Online in Last 30 Days
  - Zeigt alle Agents an, die innerhalb der letzten 7 Tage online waren.
- zz[SYS] Agent - Rebooted 14+ Days Ago
  - Zeigt alles Agents an, die innerhalb der letzten 14 Tage NICHT neu gestartet wurden.
- zz[SYS] Agent - Suspended
  - Zeigt alle angehaltenen Agents an.
- zz[SYS] Agent - User Logged On
  - Zeigt alle Rechner an, an denen ein Benutzer angemeldet ist.

Sicherheit

- zz[SYS] AV - AVG Technologies
  - Zeigt alle Rechner an, auf denen Grisoft AVG Antivirus installiert ist.
- zz[SYS] AV - Kaspersky ES
  - Zeigt alle Rechner an, auf denen Kaspersky Endpoint Security installiert ist.
- zz[SYS] AV - McAfee
  - Zeigt alle Rechner an, auf denen McAfee Antivirus installiert ist.
- zz[SYS] AV - Microsoft SE-FEP
  - Zeigt alle Rechner an, auf denen Microsoft Security Essential oder Forefront Endpoint Protection installiert ist.
- zz[SYS] AV - Sophos
  - Zeigt alle Rechner an, auf denen Sophos Antivirus installiert ist.
- zz[SYS] AV - Symantec AV
  - Zeigt alle Rechner an, auf denen Symantec Antivirus installiert ist.
- zz[SYS] AV - Symantec EP
  - Zeigt alle Rechner an, auf denen Symantec Endpoint Protection installiert ist.
- zz[SYS] AV - Trend Micro
  - Zeigt alle Rechner an, auf denen Trend Micro Antivirus installiert ist.

Backup

- **zz[SYS] Backup - CA BrightStor ARCServe**
  - Zeigt alle Rechner an, auf denen CA BrightStor ARCserve installiert ist.
- **zz[SYS] Backup - Symantec Backup Exec**
  - Zeigt alle Rechner an, auf denen Symantec Backup Exec installiert ist.

Hardware

- **zz[SYS] HW - Apple**
  - Zeigt alle Rechner des Herstellers Apple an.
- **zz[SYS] HW - Dell**
  - Zeigt alle Rechner des Herstellers Dell an.
- **zz[SYS] HW - Dell PowerEdge**
  - Zeigt alle Rechner des Herstellers Dell an, in deren Produktnamen "PowerEdge" vorkommt.
- **zz[SYS] HW - HP**
  - Zeigt alle Rechner des Herstellers HP/Hewlett Packard an.
- **zz[SYS] HW - HP ProLiant**
  - Zeigt alle Rechner des Herstellers HP/Hewlett Packard an, in deren Produktnamen "ProLiant" vorkommt.
- **zz[SYS] HW - IBM**
  - Zeigt alle Rechner des Herstellers IBM an.
- **zz[SYS] HW - IBM Series X**
  - Zeigt alle Rechner des Herstellers IBM an, in deren Produktnamen "Series X" vorkommt.
- **zz[SYS] HW - Lenovo**
  - Zeigt alle Rechner des Herstellers Lenovo an.
- **zz[SYS] HW - Not Portable**
  - Zeigt alle Rechner an, bei denen es sich nicht um tragbare Geräte handelt.
- **zz[SYS] HW - Portable**
  - Zeigt alle Rechner an, bei denen es sich um tragbare Geräte (d. h. Notebooks, Laptops, tragbare PCs, Tablet-PCs, Handhelds, Subnotebooks oder Netbooks) handelt. Hinweis: Mit Ausnahme von Mac OS X- und Linux-Rechnern.
- **zz[SYS] HW - Under 1GB Memory**
  - Zeigt alle Rechner mit weniger als 1 GB Speicher an.
- **zz[SYS] HW - Under 512MB Memory**
  - Zeigt alle Rechner mit weniger als 512 MB Speicher an.
- **zz[SYS] HW - Virtual Guest**
  - Zeigt alle Rechner an, bei denen es sich um virtualisierte Computer (VMWare-, XenServer-, VirtualBox- oder HyperV-Gäste) handelt.

Netzwerk

- **zz[SYS] Network - 10.11.12.x**
  - Zeigt alle Agents des spezifischen Netzwerk-Subnetzes 10.11.12.x an.

Betriebssystem

- **zz[SYS] OS - All Linux**
  - Zeigt alle Linux-Rechner an.
- **zz[SYS] OS - All Mac OS X**
  - Zeigt alle Rechner mit Mac OS X an.

- zz[SYS] OS - All Mac OS X Servers
  - Zeigt alle Mac OS X-Server an.
- zz[SYS] OS - All Mac OS X Workstations
  - Zeigt alle Mac OS X-Arbeitsplatzrechner an.
- zz[SYS] OS - All Servers
  - Zeigt alle Rechner mit Serverbetriebssystem an.
- zz[SYS] OS - All Windows
  - Zeigt alle Windows-Rechner an.
- zz[SYS] OS - All Windows SBS
  - Zeigt alle Windows SBS-Server an.
- zz[SYS] OS - All Windows Servers
  - Zeigt alle Windows-Server an.
- zz[SYS] OS - All Windows Workstations
  - Zeigt alle Windows-Arbeitsplatzrechner an.
- zz[SYS] OS - All Workstations
  - Zeigt alle Rechner mit einem Betriebssystem für Arbeitsplatzrechner an.
- zz[SYS] OS - Mac OS X 10.5 Leopard
  - Zeigt alle Rechner mit Mac OS X 10.5 an.
- zz[SYS] OS - Mac OS X 10.6 Snow Leopard
  - Zeigt alle Rechner mit Mac OS X 10.6 an.
- zz[SYS] OS - Mac OS X 10.7 Lion
  - Zeigt alle Rechner mit Mac OS X 10.7 an.
- zz[SYS] OS - Mac OS X 10.8 Mountain Lion
  - Zeigt alle Rechner mit Mac OS X 10.8 an.
- zz[SYS] OS - Win 2003 SBS
  - Zeigt alle Rechner mit dem Betriebssystem Windows 2003 Small Business Server (SBS) an.
- zz[SYS] OS - Win 2003 Server
  - Zeigt alle Rechner mit dem Betriebssystem Windows 2003 Server an.
- zz[SYS] OS - Win 2008 R2 Server
  - Zeigt alle Rechner mit dem Betriebssystem Windows 2008 Small Business Server an.
- zz[SYS] OS - Win 2008 SBS
  - Zeigt alle Rechner mit dem Betriebssystem Windows 2008 Server an.
- zz[SYS] OS - Win 2008 Server
  - Zeigt alle Rechner mit dem Betriebssystem Windows 2008 Server R2 an.
- zz[SYS] OS - Win 2012 Server
  - Zeigt alle Rechner mit dem Betriebssystem Windows 2012 Server an.
- zz[SYS] OS - Win 7
  - Zeigt alle Rechner mit dem Betriebssystem Windows 7 an.
- zz[SYS] OS - Win Vista
  - Zeigt alle Rechner mit dem Betriebssystem Windows Vista an.
- zz[SYS] OS - Win XP
  - Zeigt alle Rechner mit dem Betriebssystem Windows XP an.
- zz[SYS] OS - Win 8
  - Zeigt alle Rechner mit dem Betriebssystem Windows 8 an.

Patch-Verwaltung

- zz[SYS] Patch - Deny Patching Policy
    - Zeigt alle Rechner an, die zu der Patch-Richtlinie "Patchen ablehnen" gehören.
- zz[SYS] Patch - Missing 10+ Approved Patches
    - Zeigt alle Rechner an, bei denen 10 oder mehr bestätigte Patches, basierend auf ihrer Zugehörigkeit zu Patch-Richtlinie(n), fehlen.
- zz[SYS] Patch - Missing 20+ Approved Patches
    - Zeigt alle Rechner an, bei denen 20 oder mehr bestätigte Patches, basierend auf ihrer Zugehörigkeit zu Patch-Richtlinie(n), fehlen.
- zz[SYS] Patch - No Policy
    - Zeigt alle Rechner an, die nicht zu einer Patch-Richtlinie gehören.
- zz[SYS] Patch - Pending Reboot
    - Zeigt alle Rechner an, bei denen aufgrund einer vor kurzem durchgeführten Patch-Aktualisierung ein Neustart aussteht.
- zz[SYS] Patch - Scan Failed
    - Zeigt alle Rechner an, bei denen der Patch-Scan fehlgeschlagen ist.
- zz[SYS] Patch - Scan Not Scheduled
    - Zeigt alle Rechner an, denen kein Patch-Scan zugewiesen ist.
- zz[SYS] Patch - Server Patching Policy
    - Zeigt alle Rechner an, die zu der Patch-Richtlinie "Patchen von Servern" gehören.
- zz[SYS] Patch - Servers w No Policy
    - Zeigt alle Rechner an, die nicht zu einer Patch-Richtlinie gehören.
- zz[SYS] Patch - Test Patching Group
    - Zeigt alle Rechner an, die als Testsysteme für die Patch-Verwaltung vorgesehen sind.
- zz[SYS] Patch - Windows Auto Update Enabled
    - Zeigt alle Rechner an, auf denen Automatisches Windows Update aktiviert ist.
- zz[SYS] Patch - Workstation Patching Policy
    - Zeigt alle Rechner an, die zu der Patch-Richtlinie "Patchen von Arbeitsplatzrechnern" gehören.
- zz[SYS] Patch - Workstations w No Policy
    - Zeigt alle Rechner an, die nicht zu einer Patch-Richtlinie gehören.

Serverrolle

- zz[SYS] Role - Backup Exec Server
    - Zeigt alle Backup Exec-Server an.
- zz[SYS] Role - Blackberry Server
    - Zeigt alle Blackberry Enterprise-Server an.
- zz[SYS] Role - Brightstor ARCserve Server
    - Zeigt alle BrightStor ARCServe-Server an.
- zz[SYS] Role - Citrix Server
    - Zeigt alle Citrix-Server an.
- zz[SYS] Role - DHCP Server
    - Zeigt alle MS DHCP-Server an.
- zz[SYS] Role - DNS Server
    - Zeigt alle MS DNS-Server an.
- zz[SYS] Role - Domain Controller

- Zeigt alle MS AD Domain Controller-Server an.
- zz[SYS] Role - Exchange 2003 Server
  - Zeigt alle MS Exchange 2003-Server an.
- zz[SYS] Role - Exchange 2007 Server
  - Zeigt alle MS Exchange 2007-Server an.
- zz[SYS] Role - Exchange 2010 Server
  - Zeigt alle MS Exchange 2010-Server an.
- zz[SYS] Role - Exchange Server
  - Zeigt alle MS Exchange-Server an.
- zz[SYS] Role - File Server
  - Zeigt alle MS Dateiserver an.
- zz[SYS] Role - FTP Server
  - Zeigt alle MS FTP-Server an.
- zz[SYS] Role - IIS Server
  - Zeigt alle MS IIS-Server an.
- zz[SYS] Role - IMAP4 Server
  - Zeigt alle MS Exchange IMAP4-Server an.
- zz[SYS] Role - POP3 Server
  - Zeigt alle MS Exchange POP3-Server an.
- zz[SYS] Role - Print Server
  - Zeigt alle MS Druckerserver an.
- zz[SYS] Role - SharePoint Server
  - Zeigt alle MS SharePoint-Server an.
- zz[SYS] Role - SMTP Server
  - Zeigt alle MS SMTP-Server an.
- zz[SYS] Role - SQL Server
  - Zeigt alle MS SQL Server an.
- zz[SYS] Role - SQL Server 2005
  - Zeigt alle MS SQL 2005-Server an.
- zz[SYS] Role - SQL Server 2008
  - Zeigt alle MS SQL 2008-Server an.
- zz[SYS] Role - Terminal Server
  - Zeigt alle MS Terminal-Server im Anwendungsmodus an.
- zz[SYS] Role - WINS Server
  - Zeigt alle MS WINS-Server an.

Richtlinien

[System].Core.Global Policies.Agent Settings

- Agent (Core)
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Agent (Core) – Überträgt die gebräuchlichsten Agent-Einstellungen auf alle verwalteten Rechner. Das Symbol "Agent" ist aktiviert, allerdings ist nur die Option "Aktualisieren" verfügbar. Die Eincheckkontrolle ist auf 30 Sekunden gesetzt, und die

Optionen "Warnen, wenn mehrere Agents das gleiche Konto verwenden" und "Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist" sind aktiviert. Die Agent-Protokollhistorie ist für alle Protokolle auf 31 Tage gesetzt.

- **Fenster**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows
  - *Beschreibung:* Windows-Agent – Überträgt Windows-spezifische Agent-Einstellungen auf die jeweiligen Arbeitsplatzrechner. Pfad für das Arbeitsverzeichnis: c:\kworking.
- **Linux-Agent**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Linux
  - *Beschreibung:* Linux-Agent – Überträgt Linux-spezifische Agent-Einstellungen auf die jeweiligen Arbeitsplatzrechner. Pfad für das Arbeitsverzeichnis: /tmp/kworking.
- **Macintosh-Agent**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Mac OS X
  - *Beschreibung:* Macintosh-Agent – Überträgt Macintosh-spezifische Agent-Einstellungen auf die jeweiligen Arbeitsplatzrechner. Pfad für das Arbeitsverzeichnis: /Library/Kaseya/kworking.

[System].Core.Global Policies.Remote Support

- **Server-RC-Benachrichtigungsrichtlinie (Automatisch mit Administratorhinweis)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Servers
  - *Beschreibung:* Server-RC-Benachrichtigungsrichtlinie (Automatisch mit Administratorhinweis) – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Server. Benutzerbenachrichtigungstyp wird auf "Automatisch Kontrolle übernehmen" gesetzt, und die Option "Administratormitteilung für Start von Remote Control erforderlich" wird aktiviert.
- **Arbeitsplatzrechner-RC-Benachrichtigungsrichtlinie (Benachrichtigung/Beendigung mit Administratorhinweis)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Workstations
  - *Beschreibung:* Arbeitsplatzrechner-RC-Benachrichtigungsrichtlinie (Benachrichtigung/Beendigung mit Administratorhinweis) – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Arbeitsplatzrechner. Der Benutzerbenachrichtigungstyp wird auf "Benachrichtigung anzeigen, falls der Benutzer angemeldet ist‘ und "Benutzer benachrichtigen, wenn die Sitzung beendet ist" gesetzt, und die Option "Administratormitteilung für Start von Remote Control erforderlich" wird aktiviert.

[System].Core.Org Specific Policies.Agent Settings

- **Agent (Ausgeblendet)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Agent (Ausgeblendet) – Überträgt die gebräuchlichsten Agent-Einstellungen auf alle verwalteten Rechner. Das Agent-Symbol ist deaktiviert/ausgeblendet. Die Eincheckkontrolle ist auf 30 Sekunden gesetzt, und die Optionen "Warnen, wenn mehrere Agents das gleiche Konto verwenden" und "Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist" sind aktiviert. Die Agent-Protokollhistorie ist für alle Protokolle auf 31 Tage gesetzt.
- **Agent (Server)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Servers
  - *Beschreibung:* Agent (Server) – Überträgt die gebräuchlichsten Agent-Einstellungen auf alle verwalteten Server. Das Agent-Symbol wird über "Fernsteuerung deaktivieren", "Aktualisieren" und "Beenden" aktiviert. Die Eincheckkontrolle ist auf 30 Sekunden gesetzt, und die Optionen "Warnen, wenn mehrere Agents das gleiche Konto verwenden" und

"Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist" sind aktiviert. Die Agent-Protokollhistorie ist für alle Protokolle auf 93 Tage gesetzt.

- **Agent (Arbeitplatzrechner)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Workstations
  - *Beschreibung:* Agent (Arbeitplatzrechner) – Überträgt die gebräuchlichsten Agent-Einstellungen auf alle verwalteten Arbeitsplatzrechner. Das Agent-Symbol wird über "Helpdesk kontaktieren", "Fernsteuerung deaktivieren‘ und "Aktualisieren" aktiviert. Die Eincheckkontrolle ist auf 30 Sekunden gesetzt, und die Optionen "Warnen, wenn mehrere Agents das gleiche Konto verwenden" und "Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist" sind aktiviert. Die Agent-Protokollhistorie ist für alle Protokolle auf 31 Tage gesetzt.

[System].Core.Org Specific Policies.Remote Support

- **Server-RC-Benachrichtigungsrichtlinie (Automatisch ohne Administratorhinweis)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Servers
  - *Beschreibung:* Server-RC-Benachrichtigungsrichtlinie (Automatisch ohne Administratorhinweis) – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Server. Setzt den Benutzerbenachrichtigungstyp auf "Automatisch Kontrolle übernehmen‘, und erfordert keinen Administratorhinweis für den Start von Remote Control.
- **Arbeitsplatzrechner-RC-Benachrichtigungsrichtlinie (Benachrichtigung/Beendigung ohne Administratorhinweis)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Workstations
  - *Beschreibung:* Arbeitsplatzrechner-RC-Benachrichtigungsrichtlinie (Benachrichtigung/Beendigung ohne Administratorhinweis) – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Arbeitsplatzrechner. Der Benutzerbenachrichtigungstyp wird auf "Benachrichtigung anzeigen, falls der Benutzer angemeldet ist", "Benutzer benachrichtigen, wenn die Sitzung beendet ist" gesetzt, und erfordert keinen Administratorhinweis für den Start von Remote Control.
- **Arbeitplatzrechner-RC-Benachrichtigungsrichtlinie (Automatisch mit Administratorhinweis)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Workstations
  - *Beschreibung:* Arbeitsplatzrechner-RC-Benachrichtigungsrichtlinie (Automatisch mit Administratorhinweis) – Überträgt Remote Control-Benachrichtigungseinstellungen auf alle Arbeitsplatzrechner. Setzt den Benutzerbenachrichtigungstyp auf "Automatisch Kontrolle übernehmen", und erfordert einen Administratorhinweis für den Start von Remote Control.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Baseline.Baseline Audit Schedule (Annually Daytime)

- **Basisauditplan (jährlich, 1.–7. Januar, 06:00–18:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Basisauditplan (jährlich, 1.–7. Januar, 06:00–18:00 Uhr/Energiemanagement – Führt im Zeitraum vom 1. bis zum 7. Januar – jeweils zwischen 06:00 und 18:00 Uhr – auf allen bereitgestellten und eingecheckten Rechnern ein geplantes, jährliches Basis-Audit durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion, um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie kommt vor allem zum Einsatz, wenn jährliche Audits zu Planungs- oder Compliance-Zwecken erforderlich sind, und wenn für betriebliche Aufgaben ein Vergleich der Ergebnisse von "Basis"- und "Aktuell"-Audits benötigt wird. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)

- **Aktuell/SysInfo Auditplan (täglich Mo-Fr 06:00–18:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Aktuell/SysInfo Auditplan (täglich, Mo-Fr, 06:00–18:00 Uhr/Energiemanagement) – Führt auf allen Rechnern, die täglich (Mo-Fr) zwischen 06:00 und 18:00 Uhr eingecheckt sind, Audits vom Typ "Aktuell" und "Systeminformationen" durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion, um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie kommt vor allem dann zum Einsatz, wenn Kunden werktags während der Arbeitszeit Audits durchführen müssen, da die Rechner in der Regel nachts und an den Wochenenden ausgeschaltet sind. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Nighttime)

- **Aktuell/SysInfo Auditplan (täglich Mo-Fr 18:00-06:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Aktuell/SysInfo Auditplan (täglich, Mo-Fr, 18:00-06:00 Uhr/Energiemanagement) – Führt auf allen Rechnern, die täglich (Mo-Fr) zwischen 06:00 und 18:00 Uhr eingecheckt sind, Audits vom Typ "Aktuell" und "Systeminformationen" durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion, um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie wird in der Regel verwendet, wenn es der Kunde vorzieht, die Audits abends durchzuführen, wenn die Systeme weniger benutzt werden als während der Arbeitszeit und wenn die Rechner nachts entweder eingeschaltet gelassen werden oder so konfiguriert sind, dass sie mithilfe von Wake-On-LAN oder vPro-Energiemanagement aktiviert werden können, wenn sie nachts ausgeschaltet werden. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Daytime)

- **Aktuell/SysInfo Auditplan (wöchentlich Mo-Fr 06:00–18:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Aktuell/SysInfo Auditplan (wöchentlich, Mo-Fr, 06:00–18:00 Uhr/Energiemanagement) – Führt auf allen Rechnern, die wöchentlich (Mo-Fr) zwischen 06:00 und 18:00 Uhr eingecheckt sind, Audits vom Typ "Aktuell" und "Systeminformationen" durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion, um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie kommt vor allem dann zum Einsatz, wenn Kunden werktags während der Arbeitszeit Audits durchführen müssen, da die Rechner in der Regel nachts und an den Wochenenden ausgeschaltet sind. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Nighttime)

- **Aktuell/SysInfo Auditplan (wöchentlich Mo-Fr 18:00-06:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Agent_Has Checked In
  - *Beschreibung:* Aktuell/SysInfo Auditplan (wöchentlich, Mo-Fr, 18:00-06:00 Uhr/Energiemanagement) – Führt auf allen Rechnern, die wöchentlich (Mo-Fr) zwischen 18:00 und 06:00 Uhr eingecheckt sind, Audits vom Typ "Aktuell" und "Systeminformationen" durch. Zum geplanten Audit-Zeitpunkt nutzt die Richtlinie die Energiemanagementfunktion,

um vor Beginn des Audits ausgeschaltete Rechner hochzufahren. Die Richtlinie wird in der Regel verwendet, wenn es der Kunde vorzieht, die Audits abends durchzuführen, wenn die Systeme weniger benutzt werden als während der Arbeitszeit und wenn die Rechner nachts entweder eingeschaltet gelassen werden oder so konfiguriert sind, dass sie mithilfe von Wake-On-LAN oder vPro-Energiemanagement aktiviert werden können, wenn sie nachts ausgeschaltet werden. Die Richtlinie kann selektiv auf einzelne Rechner, Rechnergruppen und/oder auf ganze Rechnerorganisationen angewendet werden.

[System].Core.Org Specific Policies.Maintenance.Windows Workstation Recurring Maintenance

- **Windows Workstation-Wartung (wöchentlich, Mo-Fr 18:00-06:00 Uhr)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Workstations
  - *Beschreibung:* Windows Workstation-Wartung (wöchentlich, Mo-Fr 18:00-06:00 Uhr) – Führt wöchentlich (Mo-Fr) zwischen 18:00 und 06:00 Uhr ein geplantes Windows Workstation-Wartungsverfahren auf allen Windows Arbeitplatzrechnern durch. Wenn die Maschine zu dem Zeitpunkt nicht eingeschaltet ist, zu dem die Wartung geplant ist, überspringt die Maschine den Wartungszyklus und versucht, die Wartung eine Woche später durchzuführen.

[System].Core.Org Specific Policies.Maintenance.Macintosh Workstation Recurring Maintenance

- **Macintosh-Wartungsplan (wöchentlich Mo-Fr 18:00-06:00 Uhr)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Beschreibung:* Macintosh Workstation-Wartungsplan (wöchentlich Mo-Fr 18:00-06:00 Uhr) – Führt wöchentlich (Mo-Fr) zwischen 18:00 und 06:00 Uhr ein geplantes Macintosh-Wartungsverfahren auf allen Macintosh-Rechnern durch. Wenn die Maschine zu dem Zeitpunkt nicht eingeschaltet ist, zu dem die Wartung geplant ist, überspringt die Maschine den Wartungszyklus und versucht, die Wartung eine Woche später durchzuführen.

[System].Core.Org Specific Policies.Maintenance.Linux Recurring Maintenance

- **Linux-Wartungsplan (wöchentlich Mo-Fr 18:00-06:00 Uhr)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Linux
  - *Beschreibung:* Linux Workstation-Wartungsplan (wöchentlich Mo-Fr 18:00-06:00 Uhr) – Führt wöchentlich (Mo-Fr) zwischen 18:00 und 06:00 Uhr ein geplantes Linux-Wartungsverfahren auf allen Linux-Rechnern durch. Wenn die Maschine zu dem Zeitpunkt nicht eingeschaltet ist, zu dem die Wartung geplant ist, überspringt die Maschine den Wartungszyklus und versucht, die Wartung eine Woche später durchzuführen.

[System].Core.Org Specific Policies.Maintenance.Windows Server Recurring Maintenance

- **Windows-Serverwartung (wöchentlich So 00:00-04:00)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Servers
  - *Beschreibung:* Windows Server-Wartung (wöchentlich, So 00:00-04:00 Uhr) – Führt wöchentlich (Mo-Fr) zwischen 00:00 Uhr und 04:00 Uhr ein geplantes Windows Workstation-Wartungsverfahren auf allen Windows-Arbeitplatzrechnern durch. Wenn die Maschine zu dem Zeitpunkt nicht eingeschaltet ist, zu dem die Wartung geplant ist, überspringt die Maschine den Wartungszyklus und versucht, die Wartung eine Woche später durchzuführen.

[System].Core.Org Specific Policies.Monitoring.Server

- **Optimiertes Audit für Serverrollen**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Servers

- *Beschreibung:* Optimiertes Audit für Serverrollen – Führt wöchentlich sonntags zwischen 00:00-04:00 Uhr ein geplantes optimiertes Audit durch, um funktionale Rollen von Servern zu identifizieren, damit Monitoring-Richtlinien anhand dieser Rollen ordnungsgemäß angewendet werden können.

- **Allgemeines Windows-Server-Monitoring**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Servers
  - *Beschreibung:* Allgemeines Windows-Server-Monitoring – Wendet eine Reihe von allgemeinen Monitoringverfahren auf alle Windows-Server an. Dies umfasst mit Hardware verknüpfte Ereignisprotokolle, Windows-Dienst und allgemeines Windows-Systemleistungs-Monitoring.
- **Windows Server (Core)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Servers
  - *Beschreibung:* Windows-Server (Core) – Wendet eine Reihe von Windows Server-Core-Monitoringfunktionen auf Windows-Server an, darunter u.a. Monitoring für Standarddienste, Systemleistung, Statusberichte, Ereignisprotokolle.
- **Windows Server 2003**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_Win 2003 Server
  - *Beschreibung:* Windows Server 2003 – Wendet Standarddienst-Monitoring für Windows 2003-Server an.
- **Windows Server 2008/2008 R2**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_Win 2008 Server
  - *Beschreibung:* Windows-Server 2008/2008 R2 – Wendet Standarddienst-Monitoring für Windows 2008/2008 R2-Server an.
- **Windows Server 2012**
  - *Policy View:* zz[SYS] Policy - OS_Win 2012 Server
  - *Beschreibung:* Windows Server 2012 – Wendet Standarddienst-Monitoring für Windows 2012-Server an.

[System].Core.Org Specific Policies.Monitoring.Server.Hardware

- **Dell PowerEdge**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - HW_Dell PowerEdge
  - *Beschreibung:* Dell PowerEdge – Wendet hardwarespezifische Monitoring- und Benachrichtigungsverfahren auf Dell PowerEdge-Server an. Für dieses Monitoring müssen möglicherweise spezifische Dell PowerEdge Serververwaltungs-Werkzeuge auf dem Serverrechner installiert werden.
- **HP ProLiant**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - HW_HP ProLiant
  - *Beschreibung:* HP ProLiant – Wendet hardwarespezifische Monitoring- und Benachrichtigungsverfahren auf HP ProLiant-Server an. Für dieses Monitoring müssen möglicherweise spezifische HP ProLiant Serververwaltungs-Werkzeuge auf dem Serverrechner installiert werden.
- **IBM Series x**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - HW_IBM Series X
  - *Beschreibung:* IBM Series x – Wendet hardwarespezifische Monitoring- und Benachrichtigungsverfahren auf IBM Series X-Server an. Für dieses Monitoring müssen möglicherweise spezifische IBM Serie X Serververwaltungs-Werkzeuge auf dem Serverrechner installiert werden.

[System].Core.Org Specific Policies.Monitoring.Server.Roles

- **Backup Exec-Server**

- *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Backup Exec Server
- *Beschreibung:* Backup Exec Server – Wendet Monitoring auf Backup Exec-Server an.

- **Blackberry Enterprise Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Blackberry Server
  - *Beschreibung:* Blackberry Enterprise Server – Wendet Monitoring auf Blackberry Enterprise Server an.
- **BrightStor ARCServe Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Brightstor ARCserve Server
  - *Beschreibung:* BrightStor ARCServe Server – Wendet Monitoring auf BrightStor-Server an.
- **Citrix-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Citrix Server
  - *Beschreibung:* Citrix Server – Wendet Monitoring auf Citrix-Server an.
- **DHCP-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_DHCP Server
  - *Beschreibung:* DHCP Server – Wendet Monitoring auf DHCP-Server an.
- **DNS-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_DNS Server
  - *Beschreibung:* DNS-Server – Wendet Monitoring auf DNS-Server an.
- **Domain-Controller**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Domain Controller
  - *Beschreibung:* Domain-Controller – Wendet Monitoring auf Domain-Controller an.
- **Exchange 2003 Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Exchange 2003 Server
  - *Beschreibung:* Exchange 2003 Server – Wendet Monitoring auf Exchange 2003-Server an.
- **Exchange 2007 Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Exchange 2007 Server
  - *Beschreibung:* Exchange 2007 Server – Wendet Monitoring auf Exchange 2007-Server an.
- **Exchange 2010 Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Exchange 2010 Server
  - *Beschreibung:* Exchange 2010 Server – Wendet Monitoring auf Exchange 2010-Server an.
- **Exchange-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Exchange Server
  - *Beschreibung:* Exchange Server – Wendet Monitoring auf Exchange-Server an.
- **Dateiserver**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_File Server
  - *Beschreibung:* Dateiserver – Wendet Monitoring auf Dateiserver an.
- **FTP-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_FTP Server
  - *Beschreibung:* FTP-Server – Wendet Monitoring auf FTP-Server an.
- **IIS-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_IIS Server
  - *Beschreibung:* IIS-Server – Wendet Monitoring auf IIS-Server an.

- **IMAP4-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_IMAP4 Server
  - *Beschreibung:* IMAP4-Server – Wendet Monitoring auf IMAP4-Server an.
- **POP3-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_POP3 Server
  - *Beschreibung:* POP3-Server – Wendet Monitoring auf POP3-Server an.
- **Druckerserver**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Print Server
  - *Beschreibung:* Druckerserver – Wendet Monitoring auf Druckerserver an.
- **SharePoint Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_SharePoint Server
  - *Beschreibung:* SharePoint Server – Wendet Monitoring auf SharePoint-Server an.
- **SMTP-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_SMTP Server
  - *Beschreibung:* SMTP-Server – Wendet Monitoring auf SMTP-Server an.
- **SQL-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_SQL Server
  - *Beschreibung:* SQL-Server – Wendet Monitoring auf SQL-Server an.
- **SQL Server 2005**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_SQL Server 2005
  - *Beschreibung:* SQL-Server 2005 – Wendet Monitoring auf SQL 2005-Server an.
- **SQL Server 2008**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_SQL Server 2008
  - *Beschreibung:* SQL-Server 2008 – Wendet Monitoring auf SQL 2008-Server an.
- **Terminal-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_Terminal Server
  - *Beschreibung:* Terminal-Server – Wendet Monitoring auf Terminal-Server an.
- **WINS-Server**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Role_WINS Server
  - *Beschreibung:* WINS-Server – Wendet Monitoring auf WINS-Server an.

[System].Core.Org Specific Policies.Monitoring.Workstation

- **Allgemeines Monitoring von Windows-Arbeitsplatzrechnern**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Workstations
  - *Beschreibung:* Allgemeines Monitoring von Windows-Arbeitsplatzrechnern – Wendet allgemeine Monitor-Sets auf alle Windows-Server an. Dies umfasst mit Hardware verknüpfte Ereignisprotokolle, Windows-Dienst und allgemeines Windows-Systemleistungs-Monitoring.
- **Windows-Arbeitsplatzrechner (Core)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Workstations
  - *Beschreibung:* Windows Workstation (Core) – Wendet eine Reihe von Windows Workstation-Core-Monitoringfunktionen auf Windows-Arbeitsplatzrechner an, darunter u.a. Monitoring für Standarddienste, Systemleistung, Statusberichte, Ereignisprotokolle.
- **Windows Vista**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_Win Vista

- *Beschreibung:* Windows Vista – Wendet Standarddienst-Monitoring für Windows Vista-Rechner an.

- **Windows 7**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_Win 7
  - *Beschreibung:* Windows 7 – Wendet Standarddienst-Monitoring für Windows 7-Rechner an.
- **Windows XP**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_Win XP
  - *Beschreibung:* Windows XP – Wendet Standarddienst-Monitoring für Windows XP-Rechner an.
- **Windows 8**
  - *Policy View:* zz[SYS] Policy - OS_Win 8
  - *Beschreibung:* Windows 8 – Wendet Standarddienst-Monitoring für Windows 8-Rechner an.

[System].Core.Org Specific Policies.Monitoring.Security.Anti-Virus

- **AVG Tech**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_AVG Technologies
  - *Beschreibung:* McAfee – Wendet Monitoring für AVG Technologies AntiVirus an.
- **Kaspersky ES**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_Kaspersky ES
  - *Beschreibung:* Kaspersky ES – Wendet Monitoring für Kaspersky Endpoint Security an.
- **McAfee**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_McAfee
  - *Beschreibung:* McAfee – Wendet Monitoring für McAfee AntiVirus an.
- **Microsoft SE-FEP**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_Microsoft SE-FEP
  - *Beschreibung:* Microsoft SE-FEP – Wendet Monitoring für Microsoft Security Essentials und Forefront Endpoint Protection an.
- **Sophos**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_Sophos
  - *Beschreibung:* Sophos – Wendet Monitoring für Sophos AntiVirus an.
- **Symantec AV**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_Symantec AV
  - *Beschreibung:* Symantec – Wendet Monitoring für Symantec AntiVirus an.
- **Symantec EP**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_Symantec EP
  - *Beschreibung:* Symantec EP – Wendet Monitoring für Symantec Endpoint Protection an.
- **Trend Micro**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - AV_Trend Micro
  - *Beschreibung:* Trend Micro – Wendet Monitoring für Trend Micro AntiVirus an.

[System].Core.Org Specific Policies.Monitoring.Utility

- **Listen durch Scan aktualisieren**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows
  - *Beschreibung:* Listen durch Scan aktualisieren – Führt ein geplantes "Listen durch Scan aktualisieren" auf allen Windows-Rechnern durch, um Informationen zu

Leistungsindikatoren, Ereignisprotokollen und ausgeführten Diensten für jeden Rechner für präzise Monitoring-Zwecke auf dem neuesten Stand zu halten.

- **Monitoring Cleanup**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows
  - *Beschreibung:* Monitoring-Bereinigung – Als letzte Richtlinie, die Benachrichtigungen und Monitor-Sets enthält, stellt diese Richtlinie effektiv sicher, dass zuvor angewendete Monitoringverfahren (Ereignisprotokoll-Benachrichtigungen und Monitor-Sets, die über andere Richtlinien zugewiesen wurden und aufgrund von Rollenänderungen nicht mehr benötigt werden usw.) entfernt werden.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Common Windows Patch Mgmt Settings

- **Patch-Einstellungen ablehnen**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Deny Patching Group
  - *Beschreibung:* Patch-Einstellungen ablehnen – Wendet Einstellungen der Patch-Verwaltung auf Rechner an, die in der Ansicht "zz[SYS] Policy - Deny Patching Group" ausgewählt wurden. Legt Neustart-Aktion fest auf "Falls der Benutzer angemeldet, Neustart anfragen alle 60 Minuten bis zum Neustart. Neustart, wenn der Benutzer nicht angemeldet ist". Legt die Zugehörigkeit zur Patch-Richtlinie auf die Patch-Richtlinie ‚Patchen ablehnen" fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen' generiert wird, wenn eine "Patch-Installation fehlschlägt" oder die "Agent-Anmeldedaten ungültig sind oder fehlen".
- **Patch-Einstellungen testen**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Test Patching Group
  - *Beschreibung:* Gruppe zum Testen von Patches – Wendet Einstellungen der Patch-Verwaltung auf Rechner an, die in der Ansicht "zz[SYS] Policy - Test Patching Group" ausgewählt wurden. Legt Neustart-Aktion fest auf "Falls der Benutzer angemeldet, Neustart anfragen alle 60 Minuten bis zum Neustart. Neustart, wenn der Benutzer nicht angemeldet ist". Legt die Zugehörigkeit zur Patch-Richtlinie auf die Patch-Richtlinie "Patchen testen" fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen' generiert wird, wenn eine "Patch-Installation fehlschlägt" oder die "Agent-Anmeldedaten ungültig sind oder fehlen".
- **Automatische Windows-Aktualisierung deaktivieren**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Windows Auto Update Enabled
  - *Beschreibung:* Automatische Windows-Aktualisierung deaktivieren auf Rechnern deaktivieren, auf denen Automatisches Windows-Update aktiviert ist. Wenn Automatisches Windows-Update aktiviert wird und Patch-Management von Kaseya verwendet wird, kann das automatische Windows-Update mit der Patch-Management-Strategie von Kaseya in Konflikt geraten und zur Bereitstellung von Patches führen, die abgelehnt wurden oder für die in Kaseya noch eine Bestätigung aussteht.
- **Dateiquelle Internet**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows
  - *Beschreibung:* Dateiquelle Internet – Legt die Dateiquelle für die Patch-Verwaltung für alle Windows-Rechner auf Internet fest, sodass Patches direkt von den Microsoft-Patch- und Download-Servern heruntergeladen werden. Diese Richtlinie ist die Standardeinstellung und kann durch eine andere Richtlinie überschrieben werden, die für bestimmte Organisationen oder Rechnergruppen gilt und die Vorrang vor dieser Richtlinie hat.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings

- **Patch-Einstellungen für Workstation**

- *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Workstations
- *Beschreibung:* Workstation Patch-Einstellungen – Wendet Patch-Verwaltungseinstellungen auf Windows-Arbeitsplatzrechner an. Legt Neustart-Aktion fest auf "Falls der Benutzer angemeldet, Neustart anfragen alle 60 Minuten bis zum Neustart. Neustart, wenn der Benutzer nicht angemeldet ist". Legt Zugehörigkeit zu Patch-Richtlinie auf Patch-Richtlinie "Patchen von Workstations" fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen' generiert wird, wenn eine "Patch-Installation fehlschlägt" oder die "Agent-Anmeldedaten ungültig sind oder fehlen".

- **Täglicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mo-Fr 06:00–18:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Beschreibung:* Täglicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mo-Fr 06:00–18:00 Uhr/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien, bei denen zehn oder mehr genehmigte Patches fehlen, wöchentliche Zeitpläne für automatische Updates. Automatische Updates sind für Mo-Fr zwischen 06:00 und 18:00 Uhr geplant. Diese Richtlinie wird in der Regel verwendet, wenn bei den Rechnern des Kunden relativ viele Patches fehlen und der Kunde diese Systeme innerhalb von einigen Tagen anstatt einiger Wochen auf den neuesten Stand bringen möchte. Sobald die Rechner gepatcht sind, müssen sie nicht mehr täglich gepatcht werden. Automatische Updates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, die Energieverwaltungsoption jedoch zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.
- **Wöchentlicher Wkst.-Zeitplan (Scan Di. 06:00–18:00 Uhr/Autom. Update Mi. 6:00–18:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Beschreibung:* Wöchentlicher Wkst.-Zeitplan (Scan Di. 06:00–18:00 Uhr/Autom. Update Mi. 06:00–18:00/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien wöchentliche Zeitpläne für Patch-Scans und automatische Updates. Patch-Scans sind für dienstags zwischen 06:00 und 18:00 Uhr geplant und automatische Updates für mittwochs zwischen 06:00 und 18:00 Uhr. Diese Richtlinie wird in der Regel verwendet, wenn Kunden einen offensiveren Ansatz beim Patchen verfolgen und möchten, dass neue Patches relativ schnell auf den Rechnern bereitgestellt werden, um das Risiko durch nicht gepatchte Rechner zu senken. Automatische Updates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, die Energieverwaltungsoption jedoch zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Server Patch Mgmt Settings

- **Server-Patch-Einstellungen**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Servers
  - *Beschreibung:* Server-Patch-Einstellungen – Wendet Einstellungen der Patch-Verwaltung auf Windows-Server an. Legt Neustart-Aktion auf "Nicht neu starten nach Aktualisierung" fest, "Wenn Neustart erforderlich, E-Mail an E-Mail-Adresse zur Patch-Benachrichtigung senden." Legt Zugehörigkeit zu Patch-Richtlinie auf Patch-Richtlinie "Patchen von Servern" fest. Stellt Patch-Benachrichtigungen so ein, dass eine Benachrichtigung und eine E-Mail an die E-Mail-Adresse ‚Patch-Benachrichtigungen' generiert wird, wenn eine "Patch-Installation fehlschlägt" oder die "Agent-Anmeldedaten ungültig sind oder fehlen".
- **Wöchentlicher Serverzeitplan (Scan Mi. 18:00-06:00 Uhr)**

- *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Windows Servers
- *Beschreibung:* Wöchentlicher Serverzeitplan (Scan Mi. 18:00-06:00 Uhr) – Liefert Elementen der Server-Patch-Richtlinie einen Patch-Scan-Zeitplan. Patch-Scans sind für mittwochs zwischen 18:00 und 06:00 Uhr geplant. Bei dieser Richtlinie sind keine Implementierungen von automatischen Updates auf Servern geplant.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings

- **Dateiquellen-Systemserver**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Network_10.11.12.x
  - *Beschreibung:* Dateiquelle Systemserver – Legt die Dateiquelle für die Patch-Verwaltung für alle Windows-Rechner auf den Systemserver fest, sodass Patches zentral vom Systemserver heruntergeladen und anschließend vom Systemserver an die Rechner, die gepatcht werden, verteilt werden.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings.Other Schedules.Daytime

- **Monatlicher Wkst.-Zeitplan (Scan jeden 2. Mi. 06:00–18:00 Uhr/Autom. Update jeden 1. Mi. 06:00–18:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Beschreibung:* Monatlicher Wkst.-Zeitplan (Scan jeden 2. Mi. 06:00–18:00 Uhr/Autom. Update jeden 1. Mi. 06:00–18:00 Uhr/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien Zeitpläne für Patch-Scans und automatische Updates. Patch-Scans sind für jeden zweiten Mittwoch des Monats zwischen 06:00 und 18:00 Uhr geplant. Automatische Updates sind für jeden ersten Mittwoch des Monats zwischen 06:00 und 18:00 Uhr geplant. Diese Richtlinie kommt in der Regel zur Anwendung, wenn der Kunde einen konservativen Ansatz bei der Patch-Verwaltung verfolgt, da Scans und Updates nur einmal pro Monat durchgeführt und Updates zu Beginn des Monats bereitgestellt werden. Das bedeutet, dass die bereitgestellten Patches für mindestens einen Monat freigegeben wurden. Dadurch können die Patches vor ihrer allgemeinen Bereitstellung umfassend getestet werden. Scans und automatische Updates werden tagsüber durchgeführt, um Kunden zu bedienen, deren Rechner generell nachts ausgeschaltet sind, aber die Energieverwaltungsoption ist zu diesen Zeitpunkten aktiviert, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings.Nighttime

- **Täglicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mo-Fr 18:00-06:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Beschreibung:* Täglicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mo-Fr 18:00-06:00 Uhr/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien, bei denen zehn oder mehr genehmigte Patches fehlen, wöchentliche Zeitpläne für automatische Updates. Automatische Updates sind für Mo-Fr zwischen 18:00 und 06:00 Uhr geplant. Diese Richtlinie wird in der Regel verwendet, wenn bei den Rechnern des Kunden relativ viele Patches fehlen und der Kunde diese Systeme innerhalb von einigen Tagen anstatt einiger Wochen auf den neuesten Stand bringen möchte. Sobald die Rechner gepatcht sind, müssen sie nicht mehr täglich gepatcht werden. Automatische Updates werden abends durchgeführt, um Dienstunterbrechungen abzumildern, und zu diesen Zeitpunkten ist die Energieverwaltungsoption aktiviert, sodass ausgeschaltete Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

- **Wöchentlicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mi. 18:00-06:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Beschreibung:* Wöchentlicher Wkst.-Zeitplan für 10 oder mehr Patches (Autom. Update Mi. 18:00-06:00 Uhr/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien, bei denen zehn oder mehr genehmigte Patches fehlen, wöchentliche Zeitpläne für automatische Updates. Automatische Updates sind für mittwochs zwischen 18:00 und 06:00 Uhr geplant. Diese Richtlinie wird in der Regel verwendet, wenn bei den Rechnern des Kunden recht viele Patches fehlen und der Kunde diese Systeme innerhalb von einigen Wochen anstatt einigen Monaten auf den neuesten Stand bringen möchte. Sobald die Rechner gepatcht sind, müssen sie nicht mehr wöchentlich gepatcht werden und fallen wieder zurück in einen monatlichen Patch-Scan- und automatischen Update-Zeitplan. Automatische Updates werden abends durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, deren Energieverwaltungsoption aber zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.
- **Wöchentlicher Wkst.-Zeitplan (Scan Di. 18:00– 06:00 Uhr/Autom. Update Mi. 18:00-06:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Beschreibung:* Wöchentlicher Wkst.-Zeitplan (Scan Di. 18:00-06:00 Uhr/Autom. Update Mi. 18:00-06:00 Uhr/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien wöchentliche Zeitpläne für Patch-Scans und automatische Updates. Patch-Scans sind für dienstags zwischen 18:00 und 06:00 Uhr geplant und automatische Updates für mittwochs zwischen 18:00 und 06:00 Uhr. Diese Richtlinie wird in der Regel verwendet, wenn Kunden einen offensiveren Ansatz beim Patchen verfolgen und möchten, dass neue Patches relativ schnell auf den Rechnern bereitgestellt werden, um das Risiko durch nicht gepatchte Rechner zu senken. Scans und automatische Updates werden abends durchgeführt, um Dienstunterbrechungen abzumildern, und zu diesen Zeitpunkten ist die Energieverwaltungsoption aktiviert, sodass ausgeschaltete Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.
- **Monatlicher Wkst.-Zeitplan (Scan jeden 2. Mi. 18:00-06:00 Uhr/Autom. Update jeden 1. Mi. 18:00-06:00 Uhr/Energiemanagement)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Beschreibung:* Monatlicher Wkst.-Zeitplan (Scan jeden 2. Mi. 18:00-06:00 Uhr/Autom. Update jeden 1. Mi. 18:00-06:00 Uhr/Energiemanagement) – Liefert Elementen von Workstation-Patch-Richtlinien Zeitpläne für Patch-Scans und automatische Updates. Patch-Scans sind für jeden zweiten Mittwoch des Monats zwischen 18:00 und 06:00 Uhr geplant. Automatische Updates sind für jeden ersten Mittwoch des Monats zwischen 18:00 und 06:00 Uhr geplant. Scans und automatische Updates werden abends durchgeführt, um Dienstunterbrechungen abzumildern, und zu diesen Zeitpunkten ist die Energieverwaltungsoption aktiviert, sodass ausgeschaltete Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können. Diese Richtlinie kommt in der Regel zur Anwendung, wenn der Kunde einen konservativen Ansatz bei der Patch-Verwaltung verfolgt, da Scans und Updates nur einmal pro Monat durchgeführt und Updates zu Beginn des Monats bereitgestellt werden. Das bedeutet, dass die bereitgestellten Patches für mindestens einen Monat freigegeben wurden. Dadurch können die Patches vor ihrer allgemeinen Bereitstellung umfassend getestet werden.
- **Monatlicher Serverzeitplan (Scan 2. Mi. 18:00-06:00 Uhr)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Server Patching Policy
  - *Beschreibung:* Monatlicher Serverzeitplan (Scan 2. Mi. 18:00-06:00 Uhr) – Liefert Elementen der Server-Patch-Richtlinie einen Patch-Scan-Zeitplan. Patch-Scans sind für

jeden zweiten Mittwoch des Monats zwischen 18:00 und 06:00 Uhr geplant. Bei dieser Richtlinie sind keine Implementierungen von automatischen Updates auf Servern geplant.

- **Monatlicher Serverzeitplan (Scan 2. Mi. 18:00-06:00 Uhr/Automatisches Update 1. So. 00:00-04:00 Uhr)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - Patch_Server Patching Policy
  - *Beschreibung:* Monatlicher Serverzeitplan (Scan 2. Mi. 18:00-06:00 Uhr/Automatisches Update 1. So. 00:00-04:00 Uhr) – Liefert Elementen der Server-Patch-Richtlinie Zeitpläne für Patch-Scans und automatische Updates. Patch-Scans sind für jeden zweiten Mittwoch des Monats zwischen 06:00 und 18:00 Uhr geplant. Automatische Updates sind für jeden ersten Sonntag des Monats zwischen 00:00 und 04:00 Uhr geplant. Diese Richtlinie kommt in der Regel zur Anwendung, wenn der Kunde einen konservativen Ansatz bei der Patch-Verwaltung verfolgt, da Scans und Updates nur einmal pro Monat durchgeführt und Updates zu Beginn des Monats bereitgestellt werden. Das bedeutet, dass die bereitgestellten Patches für mindestens einen Monat freigegeben wurden. Dadurch können die Patches vor ihrer allgemeinen Bereitstellung umfassend getestet werden. Scans und automatische Updates werden frühmorgens am Wochenende durchgeführt, sodass Produktionszeit und Benutzer weniger von Dienstausfällen wegen Patchen von Servern beeinträchtigt werden.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings

- **Wöchentliches Softwareupdate von Macintosh Workstation (Installation für mittwochs 06:00–18:00:00 Uhr empfohlen)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Beschreibung:* Wöchentliches Softwareupdate von Macintosh-Workstation (Installation für mittwochs 06:00–18:00 Uhr empfohlen) – Lässt ein Mac-Softwareupdate jede Woche mittwochs zwischen 06:00 und 18:00 Uhr ausführen, bei dem empfohlene Macintosh-Softwareupdates auf Macintosh-Workstations installiert werden. Softwareupdates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, deren Energieverwaltungsoption jedoch zu diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Server Software Update Settings

- **Monatliches Softwareupdate von Macintosh-Server (Installation für 1. So. 00:00-04:00 Uhr empfohlen)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Mac OS X Servers
  - *Beschreibung:* Monatliches Softwareupdate von Macintosh-Server (Installation für 1. So. 00:00-04:00 Uhr empfohlen) – Lässt ein Mac-Softwareupdate an jedem ersten Sonntag im Monat ausführen, bei dem empfohlene Macintosh-Softwareupdates auf Macintosh-Servern installiert werden. So bleiben die Mac-Server bei den empfohlenen Aktualisierungen immer auf dem neuesten Stand.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Other Macintosh Software Update Settings

- **Monatliches Softwareupdate von Macintosh-Workstation (Installation für 1. Mi. 06:00–18:00 Uhr empfohlen)**
  - *Richtlinien-Ansicht:* zz[SYS] Richtlinie - OS_All Mac OS X Workstations
  - *Beschreibung:* Monatliches Softwareupdate von Macintosh-Workstation (Installation für 1. Mi. 06:00–18:00 Uhr empfohlen) – Lässt ein Mac-Softwareupdate an jedem ersten Mittwoch im Monat zwischen 06:00 und 18:00 Uhr ausführen, bei dem empfohlene Macintosh-Softwareupdates auf Macintosh-Workstations installiert werden. Softwareupdates werden tagsüber durchgeführt, um Kunden zu unterstützen, deren Rechner generell nachts ausgeschaltet sind, deren Energieverwaltungsoption jedoch zu

diesem Zeitpunkt aktiviert ist, sodass alle tagsüber ausgeschalteten Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

- **Monatliches Softwareupdate von Macintosh-Workstation (Installation für 1. Mi. 18:00-06:00 Uhr empfohlen)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Beschreibung:* Monatliches Softwareupdate von Macintosh-Workstation (Installation für 1. Mi. 18:00-06:00 Uhr empfohlen) – Lässt ein Mac-Softwareupdate an jedem ersten Mittwoch im Monat zwischen 18:00 und 06:00 Uhr ausführen, bei dem empfohlene Macintosh-Softwareupdates auf Macintosh-Workstations installiert werden. Softwareupdates werden abends durchgeführt, um Dienstunterbrechungen abzumildern und zu diesen Zeitpunkten ist die Energieverwaltungsoption aktiviert, sodass ausgeschaltete Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.
- **Monatliches Softwareupdate von Macintosh-Workstation (alle am 1. Mi. 18:00-06:00 Uhr installieren)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Beschreibung:* Monatliches Softwareupdate von Macintosh-Workstation (alle am 1. Mi. 18:00-06:00 Uhr installieren) – Lässt ein Mac-Softwareupdate an jedem ersten Mittwoch im Monat zwischen 18:00 und 06:00 Uhr ausführen, bei dem alle Macintosh-Softwareupdates auf Macintosh-Workstations installiert werden. Softwareupdates werden abends durchgeführt, um Dienstunterbrechungen abzumildern und zu diesen Zeitpunkten ist die Energieverwaltungsoption aktiviert, sodass ausgeschaltete Rechner vor dem Ausführen dieser Vorgänge aktiviert werden können.

[System].Core.Org Specific Policies.Patch / Update Management.Linux

- **Monatliches Update von Linux-Paket/Upgrades (Installation 1. Mi. 18:00-06:00 Uhr)**
  - *Richtlinien-Ansicht:* zz[SYS] Policy - OS_All Linux
  - *Beschreibung:* Monatliches Update von Linux-Paket/Upgrades (Installation 1. Mi. 18:00-06:00 Uhr) – Lässt ein Update-/Upgrade-Verfahren für Linux-Pakete jeden ersten Mittwoch im Monat ausführen. So sind Linux-Rechner immer aktuell und bei den verschiedenen installierten Softwarekomponenten auf dem neuesten Stand.

Details von Patch-Richtlinie

Patchen ablehnen	Standard-Bestätigungsrichtlinie
Sicherheits-Update - Kritisch (Hohe Priorität)	Abgelehnt
Sicherheits-Update - Wichtig (Hohe Priorität)	Abgelehnt
Sicherheits-Update - Mittel (Hohe Priorität)	Abgelehnt
Sicherheits-Update - Niedrig (Hohe Priorität)	Abgelehnt
Sicherheits-Update - Nicht eingestuft (Hohe Priorität)	Abgelehnt
Kritisches Update (Hohe Priorität)	Abgelehnt
Update-Rollup (Hohe Priorität)	Abgelehnt
Service-Pack (Optional - Software)	Abgelehnt
Update (Optional - Software)	Abgelehnt
Feature-Pack (Optional - Software)	Abgelehnt
Werkzeug (Optional - Software)	Abgelehnt

Patchen von Servern	
Sicherheits-Update - Kritisch (Hohe Priorität)	Bestätigung ausstehend

Sicherheits-Update - Wichtig (Hohe Priorität)	Bestätigung ausstehend
Sicherheits-Update - Mittel (Hohe Priorität)	Bestätigung ausstehend
Sicherheits-Update - Niedrig (Hohe Priorität)	Bestätigung ausstehend
Sicherheits-Update - Nicht eingestuft (Hohe Priorität)	Bestätigung ausstehend
Kritisches Update (Hohe Priorität)	Bestätigung ausstehend
Update-Rollup (Hohe Priorität)	Bestätigung ausstehend
Service-Pack (Optional - Software)	Bestätigung ausstehend
Update (Optional - Software)	Bestätigung ausstehend
Feature-Pack (Optional - Software)	Bestätigung ausstehend
Werkzeug (Optional - Software)	Bestätigung ausstehend

Patchen von Tests

Sicherheits-Update - Kritisch (Hohe Priorität)	Bestätigt
Sicherheits-Update - Wichtig (Hohe Priorität)	Bestätigt
Sicherheits-Update - Mittel (Hohe Priorität)	Bestätigt
Sicherheits-Update - Niedrig (Hohe Priorität)	Bestätigt
Sicherheits-Update - Nicht eingestuft (Hohe Priorität)	Bestätigt
Kritisches Update (Hohe Priorität)	Bestätigt
Update-Rollup (Hohe Priorität)	Bestätigung ausstehend
Service-Pack (Optional - Software)	Bestätigung ausstehend
Update (Optional - Software)	Bestätigung ausstehend
Feature-Pack (Optional - Software)	Bestätigung ausstehend
Werkzeug (Optional - Software)	Bestätigung ausstehend

Patchen von Workstations

Sicherheits-Update - Kritisch (Hohe Priorität)	Bestätigt
Sicherheits-Update - Wichtig (Hohe Priorität)	Bestätigt
Sicherheits-Update - Mittel (Hohe Priorität)	Bestätigt
Sicherheits-Update - Niedrig (Hohe Priorität)	Bestätigt
Sicherheits-Update - Nicht eingestuft (Hohe Priorität)	Bestätigt
Kritisches Update (Hohe Priorität)	Bestätigt
Update-Rollup (Hohe Priorität)	Bestätigung ausstehend
Service-Pack (Optional - Software)	Bestätigung ausstehend
Update (Optional - Software)	Bestätigung ausstehend
Feature-Pack (Optional - Software)	Bestätigung ausstehend
Werkzeug (Optional - Software)	Bestätigung ausstehend

Skripting

In diesem Abschnitt

Core.0 Common Procedures

Core.0 Common Procedures.Reboot/Shutdown/Logoff

- **Benutzerabmeldung erzwingen**
  - Meldet den gegenwärtig angemeldeten Benutzer ab.
- **Neustart: Nein abfragen**
  - Falls der Benutzer angemeldet ist, fragen Sie ihn, ob ein Neustart OK ist. Nehmen Sie nach 5 Minuten an, dass die Antwort 'Nein' lautet. Wenn der Benutzer nicht angemeldet ist, fahren Sie mit dem Neustart fort. Dieses Skript ruft 'Reboot-Ask-No-2' auf, um den Benutzer zu fragen.
- **Neustart: Nein-2 abfragen**
  - *** DIESES SKRIPT NICHT PLANEN!! ***Dieses Skript wird vom Skript "Reboot-Ask-No" aufgerufen und darf nicht von selbst geplant werden.
- **Neustart: Ja abfragen**
  - Falls der Benutzer angemeldet ist, fragen Sie ihn, ob ein Neustart OK ist. Nehmen Sie nach 5 Minuten an, dass die Antwort 'Ja' lautet. Wenn der Benutzer nicht angemeldet ist, fahren Sie mit dem Neustart fort. Dieses Skript ruft 'Reboot-Ask-Yes-2' auf, um den Benutzer zu fragen.
- **Neustart: Ja-2 abfragen**
  - *** DIESES SKRIPT NICHT PLANEN!! ***Dieses Skript wird vom Skript "Reboot-Ask-Yes" aufgerufen und darf nicht von sich selbst geplant werden.
- **Neustart erzwingen**
  - Sofortigen Neustart erzwingen.
- **Neustart-Nag**
  - Falls der Benutzer angemeldet ist, fragen Sie alle 5 Minuten nach einem Neustart, bis dieser vom Benutzer gestattet wird. Wenn der Benutzer nicht angemeldet ist, fahren Sie mit dem Neustart fort. Dieses Skript ruft 'Reboot-Nag-2' auf, um den Benutzer zu fragen.
- **Neustart-Nag-2**
  - *** DIESES SKRIPT NICHT PLANEN!! ***Dieses Skript wird vom Skript "Reboot-Nag" aufgerufen und darf nicht von sich selbst geplant werden.
- **Neustart: Kein-Benutzer**
  - Starten Sie den Rechner nur dann neu, wenn kein Benutzer angemeldet ist.
- **Neustart: Warnen**
  - Falls der Benutzer angemeldet ist, warnen Sie ihn, dass in 5 Minuter neu gestartet wird. Sollte der Benutzer nicht angemeldet sein, fahren Sie mit dem Neustart fort.
- **Neu starten – Fordert den Benutzer alle 15 Minuten zum Neustart auf, bis er mit "Ja" antwortet**
  - Dieses Skript fordert alle 15 Minuten zu einem Neustart auf.
- **Computer herunterfahren**
  - Fährt den Agent-Rechner mithilfe des Windows-Dienstprogramms shutdown.exe herunter.

Core.1 Windows-Verfahren

Core.1 Windows Procedures.Desktops.Auditing

- **BIOS-Info über WMI prüfen**
  - Nutzt WMIC, um BIOS-Info abzurufen, schreibt sie in eine Datei und ruft die Datei im Ordner "GetFile" des Systems auf, schreibt außerdem die ermittelten BIOS-Infos in das Skripting-Protokoll.
- **BOOT.INI prüfen**
  - Prüft die Inhalte von C:\BOOT.INI, falls vorhanden, schreibt einen Eintrag in das Skripting-Protokoll und ruft eine Kopie von BOOT.INI im Ordner "GetFiles" des Systems auf.
- **Dateien prüfen (alle eingegebenen Dateitypen)**
  - Sucht nach allen Dateien mit einem Satz von Dateimasken, die Sie beim Planen des Verfahrens eingeben, und erstellt eine einfache TXT-Protokolldatei und eine CSV-Datei basierend auf den eingegebenen Dateinamen. Die gefundenen Dateien werden mit vollem Pfad/Dateinamen, Datum und Uhrzeit des letzten Zugriffs, Größe in Byte, Besitzer und Dateiname aufgelistet.
    - ✓ Ausgegebene Dateien werden im Ordner #agenttemp# erstellt, der in Schritt 1 definiert wird.
    - ✓ Der Name der TXT-Protokolldatei wird durch die Variable #logfile# in Schritt 2 definiert.
    - ✓ Der Name der CSV-Datei wird durch die Variable #csvfile# in Schritt 3 definiert.
    - ✓ Die Dateimasken werden durch die Variable #filemasks# in Schritt 4 definiert.
    - ✓ Beide Ausgabedateien werden zur Überprüfung und Analyse auf den Kaseya Server unter dem Ordner "Dokumente" dieses Rechnerprofils hochgeladen.
    - ✓ Die TXT-Protokolldatei wird außerdem zur Berichterstellung in das Skriptprotokoll geschrieben.
    - ✓ Dieses Skript kann Benachrichtigungen bei Dateiänderungen auch bei einer Änderung der Schritte unterstützen.
- **Dateien prüfen (PST und OST)**
  - Sucht nach allen PST/OST-Dateien mit einem Satz von Dateimasken und erstellt eine einfache TXT-Protokolldatei- und CSV-Dateiliste, in der die gefundenen Dateien mit vollem Pfad/Dateinamen, Datum und Uhrzeit des letzten Zugriffs, Größe in Byte, Besitzer und Dateiname aufgelistet sind.
    - ✓ Ausgegebene Dateien werden im Ordner #agenttemp# erstellt, der in Schritt 1 definiert wird.
    - ✓ Der Name der TXT-Protokolldatei wird durch die Variable #logfile# in Schritt 2 definiert.
    - ✓ Der Name der CSV-Datei wird durch die Variable #csvfile# in Schritt 3 definiert.
    - ✓ Die Dateimasken werden durch die Variable #filemasks# in Schritt 4 definiert.
    - ✓ Beide Ausgabedateien werden zur Überprüfung und Analyse auf den Kaseya Server unter dem Ordner "Dokumente" dieses Rechnerprofils hochgeladen.
    - ✓ Die TXT-Protokolldatei wird außerdem zur Berichterstellung in das Skriptprotokoll geschrieben.
    - ✓ Dieses Skript kann Benachrichtigungen bei Dateiänderungen auch bei einer Änderung der Schritte unterstützen.
- **Internetgeschwindigkeit kontrollieren (WEB100CLT)**
  - Verwendet das NDT-Client-Dienstprogramm für Windows (web100clt.exe). Verbindet sich mit dem Public NDT Server, den Sie beim Ausführen/Planen des Verfahrens eingeben (eine Liste der Server finden Sie unter http://e2epi.internet2.edu/ndt/ndt-server-list.html) und führt

einen Internetgeschwindigkeitstest (Up- und Download) sowie andere Netzwerkdiagnosen durch. Die Ausgabedatei (Internet_Speed.txt) wird in den Ordner "GetFile" des Systems abgerufen.

- **IRPStackSize-Registrierungsschlüssel prüfen**
  - Prüft den Wert von IRPStackSize. Die Ereignis-ID 2011 kann von einem Antivirenprogramm und einer Vielzahl anderer Softwaretypen verursacht werden. Siehe http://support.microsoft.com/kb/177078.
- **Lokale Administratorkonten kontrollieren**
  - Protokolliert die Benutzerkonten im Skripting-Protokoll, die Teil der Administratorgruppe auf dem lokalen Rechner sind.
- **Lokale Gästekonten prüfen**
  - Protokolliert die Benutzerkonten im Skripting-Protokoll, die Teil der Gästegruppe auf dem lokalen Rechner sind. Wenn Konten ermittelt werden, werden sie aktiviert.
- **Lokale Benutzerkonten prüfen**
  - Protokolliert die Benutzerkonten im Skripting-Protokoll, die auf dem Rechner definiert sind.
- **MP3-Dateianzahl prüfen**
  - Zählt die Anzahl der auf Datenträger C: vorhandenen MP3-Dateien und trägt diese Zahl in das Skripting-Protokoll ein.
- **Offene und TCP-Überwachungsports prüfen**
  - Prüft offene und TCP-Überwachungsports in Windows mit NETSTAT und ruft dann die Ergebnisse in den Ordner "GetFile" ab.
- **PageFile-Speicherorte prüfen**
  - Prüft die PageFile-Speicherorte auf Windows-Rechnern und schreibt die Informationen in das Skripting-Protokoll.
- **Laufende Dienste prüfen (NET START)**
  - Prüft die aktuell gestarteten Dienste auf einem Windows-Rechner und ruft eine Liste dieser Dienste in den Ordner "GetFile" des Systems ab.
- **Dienste prüfen (SC QUERY)**
  - Verwendet SC QUERY, um die Liste der Windows-Dienste in einer Datei zu prüfen und die Datei in den Ordner "Get File" des Systems abzurufen.
- **Dienstregistrierungsschlüssel prüfen**
  - Fragt mit dem Befehl REG den Registrierungsschlüssel HKLM\System\CurrentControlSet\Services eines Agent ab und ruft die Ergebnisse in den Ordner "GetFile" des Systems ab.
- **Deinstallation des Registrierungsschlüssels kontrollieren**
  - Fragt mit dem Befehl REG den Registrierungsschlüssel HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall für den Rechner ab und ruft die Ergebnisse in den Ordner "GetFile" des Systems ab.
- **Plug-and-Play-USB-Geräte prüfen**
  - Verwendet VBS und WMI (Win32_PnPEntity-Klasse), um die USB-Geräte an einem Windows-Rechner zu prüfen. Ergebnisse werden in den Ordner "GetFile" des Systems abgerufen.
- **Benutzervideoauflösung**
  - Verwendet ein VBS, um die aktuelle Einstellung der Videoanzeigeauflösung des Benutzers zu prüfen. Schreibt das Ergebnis in das Skripting-Protokoll und in ein benutzerdefiniertes Systeminformationsfeld mit der Bezeichnung "Benutzervideoauflösung".
- **Windows-Monitorinformationen prüfen**

- Verwendet VBS und WMI (root\CIMV2:Win32_DesktopMonitor-Klasse), um die Windows-Monitorinformationen zu prüfen. Schreibt die Ausgabe in eine Datei und ruft die Datei in den Ordner "GetFile" des Systems ab.

- **Windows-Monitor-EDID-Informationen prüfen**
  - Ermittelt mithilfe von VBS mit WMI Monitor-EDID-Informationen (Monitorhersteller, Monitormodell und Monitorseriennummer) und schreibt die ermittelten Informationen in das Skripting-Protokoll und benutzerdefinierte Systeminformationsfelder.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS

- **Alle Freigabesitzungen und Benutzer prüfen (NET SESSION)**
  - Verwendet NET SESSION, um eine grundlegende Liste der Sitzungen auf Freigaben auf einem Agent zu sichern, und lädt sie in den Ordner Docs\Shares-NTFS hoch, sodass die Dateien über die Registerkarte "Dokumentenfunktion/Rechnerübersicht" angezeigt werden können.
- **Alle freigegebenen offenen Dateien und Benutzer prüfen (NET FILE)**
  - Verwendet NET FILE, um eine grundlegende Liste der offenen Dateien auf allen Freigaben auf einem Agent zu sichern, und lädt sie in den Ordner Docs\Shares-NTFS hoch, sodass die Dateien über die Registerkarte "Dokumentenfunktion/Rechnerübersicht" angezeigt werden können.
- **Alle Freigaben prüfen (NET SHARE)**
  - Verwendet NET SHARE, um eine grundlegende Liste der Freigaben auf einem Agent zu sichern und lädt sie in den Ordner Docs\Shares-NTFS hoch, sodass die Dateien über die Registerkarte "Dokumentenfunktion/Rechnerübersicht" angezeigt werden können.
- **Gültige Benutzer/Gruppenordnerberechtigungen prüfen (ACCESSCHK)**
  - Verwendet ACCESSCHK von Microsoft SysInternals, um die gültigen Berechtigungen eines lokalen PC/domänenbasierten Benutzers/Gruppenobjekt bei einem Ordner zu prüfen. Bearbeiten Sie dieses Skript mit den Schritten 2 bis 6 mit diesen Variablen:

    pcdom = Computername oder Domain-Name des Benutzers oder der Gruppe
    usrgrp = zu bewertender Benutzername oder Gruppenname
    drive = Buchstabe des Laufwerks, auf dem sich der Ordner befindet
    folder = vollständiger Pfad des zu prüfenden Ordners
    fldrdesc = ein beschreibender Name des zu prüfenden Ordners (ohne Sonderzeichen)
- **Nicht-Admin-Freigaben prüfen (SRVCHECK)**
  - Verwendet SRVCHECK, um eine grundlegende Liste der Nicht-Admin-Freigaben auf einem Agent zu sichern, und lädt sie in den Ordner Docs\Shares-NTFS hoch, sodass die Dateien über die Registerkarte "Dokumentenfunktion/Rechnerübersicht" angezeigt werden können.
- **Freigegebene Ordner prüfen (DUMPSEC)**
  - Verwendet DUMPSEC, um einen Bericht über alle Freigaben mit ihren Pfaden, Konten, Besitzern und Zugriffsberechtigungen zu erstellen, und lädt sie in den Ordner Docs/Shares-NTFS hoch, sodass die Dateien über die Registerkarte "Dokumentenfunktion/Rechnerübersicht" angezeigt werden können.
- **Freigegebene Ordner und ACLs prüfen (VBS/WMI)**
  - Prüft alle lokalen Freigaben, Freigabe- und NTFS-Berechtigungen mithilfe eines VBS mit WMI.
- **Freigegebene Drucker prüfen (DUMPSEC)**
  - Verwendet DUMPSEC, um einen Bericht über alle Drucker mit Namen, Konten, Besitzern und Zugriffsberechtigungen zu erstellen, und lädt sie in den Ordner Docs/Shares-NTFS hoch, sodass die Dateien über die Registerkarte "Dokumentenfunktion/Rechnerübersicht" angezeigt werden können.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS.Audit Admin Shares

- **Automatische Admin-Freigaben prüfen**
  - Verwendet NET SHARE, um automatische Admin-Freigaben wie C$ usw. zu prüfen. Die Ergebnisse werden in den Systemordner "Dokumente" in einen Freigabe-NFTS-Unterordner abgerufen.
- **Automatische Admin-Freigabeneinstellungen prüfen**
  - Auf Grundlage des Betriebssystems des Rechners wird das Vorhandensein und der Wert von AutoShareServer oder AutoShareWkst in der Windows-Registry geprüft und ein Eintrag im Skripting-Protokoll verfasst, der angibt, ob diese Funktion aktiviert oder deaktiviert ist.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Dell

- **Inventarisierung der Dell BIOS-Einstellungen über DCCU**
  - Verwendet das Dell Client Configuration Utility (DCCU), um eine Inventarisierung des BIOS eines Dell Rechners der Unternehmensklasse vorzunehmen. Die Ergebnisse werden in den Ordner "GetFile" des Systems abgerufen.
- **Dell BIOS-Einstellungen über DCCU einstellen**
  - Stellt die Dell BIOS-Einstellungen auf Grundlage der bei Planung gelieferten Einstellung und Werte ein. Das Format für die gelieferte Dell BIOS-Einstellung muss dem Format entsprechen, das das Dell Client Configuration Utility (DCCU) verwendet.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.HP

- **HP BiosConfigUtility GetConfig**
  - Verwendet das HP Bios Config Utility, um eine Inventarisierung des BIOS eines HP Rechners der Unternehmensklasse vorzunehmen. Die Ergebnisse werden in den Ordner "GetFile" des Systems abgerufen.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Lenovo

- **Lenovo BIOS-Einstellungen über WMI-VBS abrufen**
  - Verwendet VBS und WMI, um alle BIOS-Einstellungen auf Lenovo-Systemen abzurufen.
- **Lenovo BIOS-Einstellungen über WMI-VBS einstellen**
  - Verwendet VBS und WMI, um die BIOS-Einstellungen auf Lenovo-Systemen zu konfigurieren. Fragt bei Ausführung/Planung nach dem Lenovo BIOS-Einstellungsnamen.

Core.1 Windows Procedures.Desktops.Machine Control.File Sharing

- **Einfache Dateifreigabe bei Windows XP deaktivieren (Sets ForceGuest=0)**
  - Deaktiviert die Funktion zur einfachen Dateifreigabe (Sets ForceGuest=0) bei Windows XP-Systemen. Stoppt danach den Serverdienst und startet ihn neu, sodass die Änderung wirksam wird.
- **Automatische Admin-Freigaben aktivieren**
  - Aktiviert die Funktion "AutoshareWks" bei Windows-Workstations, sodass Admin-Freigaben automatisch erstellt werden, wenn der Serverdienst startet. Diese Agent-Prozedur startet NICHT den Serverdienst (lanmanserver) neu.
- **Einfache Dateifreigabe aktivieren (Sets ForceGuest=1) bei Windows XP**
  - Aktiviert die Funktion zur einfachen Dateifreigabe (Sets ForceGuest=1) bei Windows XP-Systemen. Stoppt danach den Serverdienst und startet ihn neu, sodass die Änderung wirksam wird.
- **Automatische Admin-Freigaben deaktivieren**
  - Deaktiviert die Funktion "AutoshareWks" bei Windows-Workstations, sodass Admin-Freigaben automatisch erstellt werden, wenn der Serverdienst startet. Diese Agent-Prozedur startet NICHT den Serverdienst (lanmanserver) neu.

Core.1 Windows Procedures.Desktops.Machine Control.File System

- **Dateisystem auf Laufwerk in NTFS konvertieren**
  - Konvertiert das Dateisystemformat auf dem Systemlaufwerk (d. h. die Startpartition) von FAT/FAT32 in NTFS. Dies funktioniert nur bei Betriebssystemen, die NTFS unterstützen (Windows NT4 / 2000 / XP / 2003 / Vista)
- **Dateien anhand des Änderungsdatums löschen**
  - Fragt nach dem Alter der zu löschenden Dateien, dem vollständigen Laufwerk/Pfad zum Starten des Löschvorgangs und nach einer zu löschenden Dateimaske. Verwendet dann FORFILES, um rekursiv alle Ordner unter dem angegebenen vollständigen Laufwerk/Pfad zu verarbeiten, und löscht die Dateien, die der Dateimaske entsprechen, wenn sie älter als das angegebene Alter sind.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Block Websites

- **"Beliebige" Website blockieren**
  - Dieses Skript bearbeitet die Windows-Hostdateien und zeigt eine beliebige Website, die Sie in der Aufforderung an Localhost eingeben, wobei der Zugriff auf diese Website von diesem Endpunkt aus blockiert wird. Dies kann für Arbeitgeber nützlich sein, die die Produktivität steigern möchten, oder für Heiterkeit sorgen.
- **Alle blockierten Websites löschen**
  - Wird verwendet, um alle Bearbeitungen von Windows-Hostdateien zu entfernen. Aktualisiert die Standardeinstellungen für Hostdateien.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Diagnostics

- **Netzwerkdiagnosetest (NETSH)**
  - Verwendet NETSH, um einen Netzwerkdiagnosetest durchzuführen und ruft die Ergebnisse in den Ordner "Dokumente" des Systems in einen Unterordner namens "Netzwerkdiagnose" ab.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Network Connection

- **LAN-Verbindung zur Verwendung von DHCP konfigurieren**
  - Verwendet NETSH, um die Konfiguration der von Windows als "LAN-Verbindung" bezeichneten Netzwerkverbindung zu ändern, sodass sie DHCP für ihre IP-Adresse, DNS und WINS-Einstellungen verwendet.
- **RAS-DNS-Priorität korrigieren**
  - Korrigiert das Problem der RAS-DNS-Bindungspriorität, wie in http://support.microsoft.com/kb/311218/en-us beschrieben.
- **Windows-IP-Konfiguration abrufen (IPCONFIG /ALL)**
  - Verwendet IPCONFIG /ALL, um die IP-Adressenkonfiguration aller aktivierten Netzwerkverbindungen auf einem Windows-Rechner abzurufen. Die Ergebnisse werden in den Ordner "GetFiles" des Systems abgerufen.
- **IP-Adresse freigeben und erneuern**
  - Verwendet eine Batch-Datei, um die IP-Adresse eines Windows-Rechners freizugeben und zu erneuern.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Dell

- **Wake-On-LAN in Dell BIOS aktivieren (DCCU)**
  - Verwendet das Dell Client Configuration Utility (DCCU), um Wake-On-LAN im BIOS von Dell Rechnern der Unternehmensklasse zu aktivieren.
- **Wake-On-LAN in Dell BIOS aktivieren (CCTK)**
  - Verwendet das Dell Client Configuration Tool Kit (DCCU), um Wake-On-LAN im BIOS von Dell Rechnern der Unternehmensklasse zu aktivieren.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.HP

- **Wake-On-LAN in HP BIOS aktivieren**
  - Verwendet das HP BIOS Configuration Utility, um Wake-On-LAN im BIOS von HP Rechnern der Unternehmensklasse zu aktivieren.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Lenovo

- **Wake-On-LAN in Lenovo BIOS aktivieren**
  - Verwendet VBS und WMI, um Wake-On-LAN im BIOS von Lenovo Rechnern der Unternehmensklasse zu aktivieren.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Windows

- **Wake-On-LAN in Windows für alle NICs aktivieren**
  - Verwendet VBS, um die Wake-On-LAN-Funktion der Energieverwaltung auf jeder Windows-Netzwerkschnittstelle zu aktivieren. Dadurch kann der Rechner im Ruhezustand oder Standby-Modus über ein Magic Packet aktiviert werden. Außerdem müssen WOL-Funktionen auch im BIOS aktiviert sein, damit WOL funktioniert.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wireless

- **Drahtlose Netzwerkgeräte deaktivieren**
  - Verwendet DEVCON.EXE, um drahtlose Netzwerkgeräte in einem Windows-System zu deaktivieren
- **Drahtlose Netzwerkgeräte aktivieren**
  - Verwendet DEVCON.EXE, um drahtlose Netzwerkgeräte in einem Windows-System zu aktivieren
- **NIC bei drahtloser Netzwerkverbindung deaktivieren**
  - Verwendet NETSH, um die Netzwerkschnittstellenkarte (NIC) zu deaktivieren, die der von Windows als "Drahtlosnetzwerkverbindung" bezeichneten Netzwerkverbindung zugeordnet ist.
- **NIC bei drahtloser Netzwerkverbindung aktivieren**
  - Verwendet NETSH, um die Netzwerkschnittstellenkarte (NIC) zu aktivieren, die der von Windows als "Drahtlosnetzwerkverbindung" bezeichneten Netzwerkverbindung zugeordnet ist.

Core.1 Windows Procedures.Desktops.Machine Control.Reboot/Shutdown

- **Jetzt Ruhezustand**
  - Veranlasst einen Windows-Rechner, sofort in den Ruhezustand zu gehen
- **Jetzt Standby**
  - Veranlasst einen Windows-Rechner, sofort in den Standby-Modus zu gehen
- **Abbrechen durch Herunterfahren**
  - Fahren Sie den Computer mit Shutdown.exe herunter
- **Herunterfahren in 60 Sekunden**
  - Fährt den Computer mit Shutdown.exe nach 60 Sekunden herunter
- **Desktop sperren**
  - Sperrt den Desktop eines Windows-Rechners; zum Entsperren des Desktops muss der aktuell angemeldete Benutzer erneut seine Anmeldedaten eingeben.

Core.1 Windows Procedures.Desktops.Machine Control.System Restore

- **Alle Systemwiederherstellungspunkte auflisten**
  - Verwendet WMIC, um alle Systemwiederherstellungspunkte aufzuzählen und ruft die Liste in den Ordner "Get File" des Systems ab.

- **Systemwiederherstellung auf allen Laufwerken aktivieren**
  - Verwendet DISKPART, um alle lokalen Partitionen aufzuzählen und gibt diese Laufwerkliste in WMIC ein, um die Systemwiederherstellung auf jedem Datenträger zu deaktivieren. Dadurch werden alle vorhandenen Systemwiederherstellungspunkte entfernt.
- **Systemwiederherstellung aller Laufwerke deaktivieren**
  - Verwendet DISKPART, um alle lokalen Partitionen aufzuzählen und gibt diese Laufwerkliste in WMIC ein, um die Systemwiederherstellung auf jedem Datenträger zu deaktivieren. Dadurch werden alle vorhandenen Systemwiederherstellungspunkte entfernt.
- **Benannten Systemwiederherstellungspunkt erstellen**
  - Verwendet WMIC, um einen Systemwiederherstellungspunkt zu erstellen

Core.1 Windows Procedures.Desktops.Machine Control.Trusted Sites

- **Vertrauenswürdige Sites hinzufügen**
  - Führt ein Registry-Verfahren auf dem Rechner aus, damit alle Elemente der Domäne ActiveX ausführen können. In diesem Beispiel wird Kaseya.net hinzugefügt

Core.1 Windows Procedures.Desktops.Machine Control.USB/Disk Drive Control

- **USB-Laufwerke deaktivieren**
  - **Nach Änderung durch Skript muss Endpunkt neu gestartet werden**Es gibt eine kleine Änderung an der Registry, wodurch die USB-Speichertreiber nicht beim Systemstart starten. Verhindert, dass Personen sich an den Rechner setzen und Daten auf einen USB-Stick kopieren, aber ermöglicht es Ihnen, weiterhin Scanner, Tastatur und Maus zu verwenden.
  - Denken Sie wie immer daran, Ihr System zu sichern, bevor Sie Änderungen an der Registry vornehmen. Öffnen Sie "regedit" und navigieren Sie zu diesem Schlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Beachten Sie den Wert "Start". Wenn Sie diesen Wert auf 4 ändern, werden USB-Speichergeräte deaktiviert. Ändern Sie diesen Wert auf 3 und USB-Speichergeräte werden aktiviert.
- **USB-Laufwerke aktivieren**
  - **Nach Änderung durch Skript muss Endpunkt neu gestartet werden**Es gibt eine kleine Änderung an der Registry, wodurch die USB-Speichertreiber nicht beim Systemstart starten. Verhindert, dass Personen sich an den Rechner setzen und Daten auf einen USB-Stick kopieren, aber ermöglicht es Ihnen, weiterhin Scanner, Tastatur und Maus zu verwenden.
  - Denken Sie wie immer daran, Ihr System zu sichern, bevor Sie Änderungen an der Registry vornehmen. Öffnen Sie "regedit" und navigieren Sie zu diesem Schlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Beachten Sie den Wert "Start". Wenn Sie diesen Wert auf 4 ändern, werden USB-Speichergeräte deaktiviert. Ändern Sie diesen Wert auf 3 und USB-Speichergeräte werden aktiviert.
- **Schreibschutz von USB-Laufwerken deaktivieren**
  - Deaktiviert den Schreibschutz bei USB-Geräten auf Windows-Rechnern mit einem Betriebssystem ab XP SP2 (siehe http://technet.microsoft.com/en-us/library/bb457157.aspx).
- **Schreibschutz von USB-Laufwerken aktivieren**
  - Aktiviert den Schreibschutz bei USB-Geräten auf Windows-Rechnern mit einem Betriebssystem ab XP SP2 (siehe http://technet.microsoft.com/en-us/library/bb457157.aspx).
- **Optische CD-ROM-Laufwerke deaktivieren**
  - Deaktiviert CD-ROM-Laufwerkgeräte
- **CD-ROM-Laufwerke aktivieren**
  - Aktiviert CD-ROM-Laufwerkgeräte
- **Diskettengeräte mit hoher Kapazität deaktivieren**

- Deaktiviert Diskettengeräte mit hoher Kapazität
- **Diskettengeräte mit hoher Kapazität aktivieren**
  - Aktiviert Diskettengeräte mit hoher Kapazität
- **Diskettenlaufwerk deaktivieren**
  - Deaktiviert Diskettengeräte
- **Diskettenlaufwerk aktivieren**
  - Aktiviert Diskettengeräte
- **Desktop-Zugriff beschränken**
  - Beschränkt den Zugriff auf den "Desktop" im Explorer. Der "Desktop" wird leer angezeigt und Benutzer können nicht darauf zugreifen.
- **Beschränkung von Desktop-Zugriff aufheben**
  - Beschränkt den Zugriff auf den "Desktop" im Explorer. Der "Desktop" wird leer angezeigt und Benutzer können nicht darauf zugreifen.
- **Zugriff auf alle Laufwerke (A–Z) in Explorer ausblenden und beschränken**
  - Verwendet die Registry-Einstellungen "NoViewOnDrive" und "NoDrives", um den Zugriff auf alle Laufwerksbuchstabe A–Z in einem Windows-Rechner auszublenden und zu beschränken.
- **Zugriff auf Laufwerke C und D in Explorer ausblenden und beschränken**
  - Sie können "Nur C blockieren" oder "Nur D blockieren" oder "Alle Laufwerke blockieren" mit einem der "01.Block"-Verfahren auswählen
- **Zugriff auf beliebige Liste an Laufwerken in Explorer ausblenden und beschränken**
  - Sie können "Nur C blockieren" oder "Nur D blockieren" oder "Alle Laufwerke blockieren" mit einem der "01.Block"-Verfahren auswählen
- **Zugriff auf alle Laufwerke (A-Z) in Explorer einblenden und Beschränkung aufheben**
  - Entfernt vorherige Laufwerkzugriffsbeschränkungen, die möglicherweise vorhanden sind.
  - Hinweis: Windows unterstützt die Fähigkeit, Zugriff zu blockieren, um verschiedene Laufwerksbuchstaben innerhalb von Explorer anzuzeigen. Durch diese Einschränkung können Benutzer Arbeitsplatz oder Explorer nicht verwenden, um auf den Inhalt der ausgewählten Laufwerke zuzugreifen. Sie können auch nicht Ausführen, Netzlaufwerk zuordnen oder den Befehl "Dir" verwenden, um die Verzeichnisse in diesen Laufwerken anzuzeigen. Diese Agent-Prozedur entfernt jegliche Einschränkung auf dieses Ergebnis.

Core.1 Windows Procedures.Desktops.Machine Control.User Access Control

- **Legt die Benutzerzugriffssteuerung (UAC) fest auf "Immer Benachrichtigen"**
  - Legt die Benutzerzugriffssteuerung in Windows Vista, Windows 7 und Windows 8 auf "Immer Benachrichtigen" fest.
- **Legt die Benutzerzugriffssteuerung (UAC) fest auf "Standardmäßig Benachrichtigen"**
  - Legt die Benutzerzugriffssteuerung in Windows Vista, Windows 7 und Windows 8 auf "Standardmäßig Benachrichtigen" fest.
- **Legt die Benutzerzugriffssteuerung (UAC) fest auf "Unsicher benachrichtigen"**
  - Legt die Benutzerzugriffssteuerung fest auf "Unsicher benachrichtigen" in Windows Vista, Windows 7 und Windows 8.
- **Legt die Benutzerzugriffssteuerung (UAC) fest auf "Nie benachrichtigen"**
  - Deaktiviert die Benutzerzugriffssteuerung in Windows Vista, Windows 7 und Windows 8.

Core.1 Windows Procedures.Desktops.Machine Control.Windows Configuration

- **Blendet ein Konto vom Windows Anmeldebildschirm "Schnelle Benutzerumschaltung" aus**

  - Dieses Skript fügt einen DWORD-Wert hinzu, wobei der Wert "support user" und Daten auf 0 gesetzt ist. Nach einem Neustart zeigt der PC "support user" nicht mehr im Willkommensbildschirm an.
- **Blendet ein Konto vom Windows Anmeldebildschirm Schnelle Benutzerumschaltung ein**
  - Dieses Skript fügt einen DWORD-Wert hinzu, wobei der Wert "support user" und Daten auf 0 gesetzt ist. Nach einem Neustart zeigt der PC "support user" nicht mehr im Willkommensbildschirm an.
- **Ausgeblendete Betriebssystemdateien deaktivieren**
  - Deaktiviert die Option "Ausgeblendete Betriebssystemdateien" in Windows Explorer.
- **Anzeigen der Inhalte der Systemordner aktivieren**
  - Aktiviert die Option "Inhalt von Systemordnern anzeigen" in Windows Explorer.
- **"Erweiterungen für bekannte Dateitypen ausblenden" aktivieren**
  - Aktiviert die Option "Erweiterungen für bekannte Dateitypen ausblenden" in Windows Explorer.
- **"Ausgeblendete Dateien und Ordner anzeigen" aktivieren**
  - Aktiviert die Option "Ausgeblendete Dateien und Ordner anzeigen" in Windows.
- **Minimale Passwortlänge von 8 Zeichen in Windows erzwingen**
  - Zwingt Windows, Kennwörter unter einer bestimmten Mindestlänge abzulehnen. So kann verhindert werden, dass Benutzer zu einfache Kennwörter verwenden, wenn Sicherheit von Bedeutung ist. Fügen Sie einen neuen REG_BINARY-Wert von "MinPwdLen" hinzu und stellen Sie die Daten auf die Mindestzahl von erforderlichen Zeichen ein, damit ein Kennwort akzeptiert wird. Das folgende Beispiel ist 8. Hinweis: Dies wirkt sich nicht auf vorhandene Kennwörter aus, sondern nur auf neue oder geänderte Kennwörter.
- **Ballon-Pop-ups für aktuellen Windows-Benutzer unterdrücken**
  - Unterdrückt alle Ballon-Pop-ups in Windows für den angemeldeten Benutzer. Siehe http://msdn.microsoft.com/en-us/library/ms940877(v=winembedded.5).aspx

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Check Disk

- **Disk überprüfen Alle Laufwerke**
  - Verwendet DISKPART, um alle lokalen Partitionen aufzuzählen, und gibt diese Laufwerkliste in CHKDSK ein, um jeden Datenträger zu reparieren.
- **Disk prüfen Systemlaufwerk (Planen beim nächsten Neustart)**
  - Führt einen CHKDSK-Befehl im Systemlaufwerk aus. Die Ergebnisse der Wartung werden durch das Skript "Disk Verify prüfen" bewertet.
- **Disk prüfen Systemlaufwerk (nur Analyse)**
  - Führt einen CHKDSK-Befehl im Systemlaufwerk aus. Die Ergebnisse der Wartung werden bewertet, ein Protokolleintrag wird in dem Skripting-Protokoll mit den Ergebnissen gespeichert, und die Ergebnisse werden in den Systemordner "Datei abrufen" abgerufen.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Defragmentation

- **Alle Laufwerke defragmentieren**
  - Verwendet DISKPART, um alle lokalen Partitionen aufzuzählen, und gibt diese Laufwerkliste in DEFRAG ein, um jeden Datenträger zu optimieren. Ruft DEFRAG-Ergebnisse für alle Laufwerke in den Ordner "GetFile‘ ab.
- **Systemlaufwerk defragmentieren (nur Analyse)**
  - Führt eine Defragmentationsanalyse im Systemlaufwerk in Windows durch (üblicherweise C:). Defragmentationsergebnisse werden in dem Skripting-Protokoll gespeichert.
- **Seitendatei defragmentieren & Registry**

- Verwenden Sie das Dienstprogramm PageDefrag von Sysinternals, um die System-Seitendatei und Registry zu defragmentieren und führen Sie einen Neustart durch (nur Windows XP).

- **Systemlaufwerk defragmentieren (Analyse & Benutzer auffordern, wenn erforderlich)**
  - Führt eine Defragmentationsanalyse im Systemlaufwerk in Windows durch (üblicherweise C:). Defragmentationsergebnisse werden in dem Skripting-Protokoll gespeichert. Wenn ein Benutzer am Rechner angemeldet ist, wird er vom Verfahren gefragt, ob eine vollständige Defragmentierung des Laufwerks durchgeführt werden soll und führt diese aus, wenn der Benutzer mit Ja antwortet.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Disk Cleanup

- **Windows Disk-Bereinigung**
  - Legt die "sageset"-Registrierungseinträge für cleanmgr.exe fest und führt dann die Datei cleanmgr.exe mit dem Parameter "sagerun" aus, um Dateien an den folgenden Speicherorten automatisch zu bereinigen: Aktiver Setup Temporärer Ordner Inhaltsindizierung Bereiniger Heruntergeladene Programmdateien Internet-Cache-Dateien Speicherauszug Alte ChkDsk-Dateien Papierkorb Remote-Desktop-Cache-Dateien Setup-Protokolldateien Temporäre Dateien Temporäre Offline-Dateien WebClient und WebPublisher Cache

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Flush DNS

- **DNS-Resolver-Cache leeren**
  - Leert die Inhalte des DNS-Client-Resolver-Cache und setzt diese zurück, indem IPCONFIG /FLUSHDNS ausgeführt wird

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.IE Files Management

- **Internet Explorer-Cookies löschen**
  - Löscht die Internet Explorer-Cookies für den gegenwärtig angemeldeten Benutzer.
- **Internet Explorer-Formulardaten löschen**
  - Löscht die Internet Explorer-Formulardaten für den gegenwärtig angemeldeten Benutzer.
- **Internet Explorer-Historie löschen**
  - Löscht den Internet Explorer-Verlauf für den gegenwärtig angemeldeten Benutzer.
- **Internet Explorer-Kennwörter löschen**
  - Löscht die Internet Explorer-Kennwörter für den gegenwärtig angemeldeten Benutzer.
- **Temporäte Internet Explorer-Dateien löschen**
  - Löscht die temporären Dateien des Internet Explorer für den gegenwärtig angemeldeten Benutzer.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Systemwiederherstellungspunkt für wöchentliche Desktop-Wartung erstellen**
  - Verwendet WMIC, um einen Systemwiederherstellungspunkt mit dem Namen "Wöchentliche Desktop-Wartung" zu erstellen. Dieses Skripting kann zu Beginn des wöchentlichen Wartungsverfahrens des Arbeitplatzrechners aufgerufen werden.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Systemwiederherstellungspunkt der Patch-Verwaltung erstellen**

- Verwendet WMIC, um einen Systemwiederherstellungspunkt mit dem Namen "Patch-Verwaltung" zu erstellen. Dieses Skripting kann vor einer Patch-Bereitstellung durch eine Pre-Agent-Prozedur für automatische Updates aufgerufen werden.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.TEMP Files

- **TEMP-Ordner des Benutzers löschen**
  - Löscht alle Dateien und Ordner innerhalb und unterhalb des %TEMP%-Ordners des angemeldeten Benutzers, die nicht aktuell durch Windows gesperrt/geöffnet sind.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Time Sync

- **Zeit synchronisieren via SNTP**
  - Stellt die Windows-Uhr auf die Zeit von time.windows.com ein

Core.1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance

- **Wöchentliche Wartung des Arbeitplatzrechners**
  - Führt alle wöchentlichen Desktop-Wartungsaufgaben durch, plant das Ausführen des Skripts während des Wartungsfensters.

Core.1 Windows Procedures.Desktops.Maintenance.Maintenance Notifications

- **Erinnerung für wöchentliche Desktop-Wartung**
  - Dieses Skript ist tagsüber für die Ausführung vor der Desktop-Patchen-Wartung vorgesehen. Sendet eine Nachricht an einen Desktop-Endbenutzer, die angibt, dass der Rechner über Nacht laufen soll.

Core.1 Windows Procedures.Desktops.Software Control.Internet Explorer

- **Standard-Internet Explorer-Startseite einstellen**
  - Stellen Sie die Standardseite in Internet Explorer ein. Ändern Sie die Site einfach in Schritt 1.

Core.1 Windows Procedures.Desktops.Software Control.Windows Firewall

- **Windows Firewall deaktivieren**
  - Verwendet NETSH, um die Windows Firewall zu deaktivieren

Core.1 Windows Procedures.Servers.Active Directory.AD Replication

- **AD-Replikationsprüfung mit REPADMIN durchführen**
  - Führt eine Replikationsprüfung von Active Directory-Diensten mithilfe des Dienstprogramms REPADMIN aus. Sendet Ergebnisse per E-Mail; Sie MÜSSEN die E-Mail-Adresse aktualisieren, um die Ergebnisse zu erhalten.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2003

- **ExBPA Report 2003 Server**
  - Entwickelt für Exchange 2003. Verwendet den Exchange Best Practice Analyzer, um einen Bericht von allen Fehlern zu erstellen. MS Logparser 2.0 wird anschließend verwendet, um die Ergebnisse zu analysieren und einen abschließenden Bericht an die E-Mail-Adresse des Administrators zu senden, der das Skripting ausführt/plant. Der Exchange Best Practice Analyzer muss vor der Verwendung dieses Skriptings installiert werden.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2007

- **ExBPA Report 2007 Server**
  - Entwickelt für Exchange 2007. Verwendet den Exchange Best Practice Analyzer, um einen Bericht von allen Fehlern zu erstellen. MS Logparser 2.0 wird anschließend verwendet, um

die Ergebnisse zu analysieren und einen abschließenden Bericht an die E-Mail-Adresse des Administrators zu senden, der das Skripting ausführt/plant. Der Exchange Best Practice Analyzer muss vor der Verwendung dieses Skriptings installiert werden.

Core.1 Windows Procedures.Servers.IIS Server

- **Einen IISRESET auf IIS-Server durchführen**
  - Führt einen IISReset auf dem Rechner durch.

Core.1 Windows Procedures.Servers.Maintenance

- **Wöchentliche Serverwartung**
  - Führt alle wöchentlichen Desktop-Wartungsaufgaben durch.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Disk Usage

- **DiskUsage.GetDirTree.C-D-E-F-G-M-N**
  - Gibt die Festplattennutzung auf den Laufwerken C, D, E, F, G, M und N aus. Schreibt die Disk-Nutzungsstrukturergebnisse in das Skripting-Protokoll. Nicht vorhandene Laufwerke zeigen keine Disk-Nutzungsergebnisse an.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Get Process List

- **Leistung. Prozessliste abrufen**
  - Verwendet kperfmon.exe, um Prozessliste, CPU % und Speicherverbrauch zu erhalten. Dieses Skript kann für die Ausführung konfiguriert werden, wenn die Leistungs-Monitorzähler einen Alarm auslösen. Speichert Ergebnisse im Skripting-Protokoll.

Core.1 Windows Procedures.Servers.Print Server

- **Warteschlange Druckerspooler löschen**
  - Hält den Druck-Spooler an, löscht Warteschlangen und startet den Druck-Spooler neu.

Core.1 Windows Procedures.Servers.Service Control Manager

- **SCM kompilieren**
  - Kompiliert den Dienststeuerungs-Manager erneut, um sicherzustellen, dass SCM-Ereignisse im Systemprotokoll gespeichert werden.

Core.1 Windows Procedures.Servers.Terminal Server

- **Terminal Server – Abmeldung getrennte Sitzungen**
  - Meldet alle getrennten Sitzungen eines Terminal-Servers ab.
- **Terminal-Server – Abmeldung Sitzung X**
  - Referenz-URL: http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Terminal Server – Sitzung 1 abmelden**
  - Referenz-URL: http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Terminal-Server – Abfragesitzungen**
  - Verwendet QUERY USER, um eine Liste aller Terminal-Server-Sitzungen zu erstellen und schreibt die Sitzungsinformationsliste in das Skripting-Protokoll.
- **Terminal-Server – Neu starten in 60 Sekunden**
  - Startet einen Terminal-Server neu; angemeldete Benutzer haben 60 Sekunden Zeit, um Anwendungen zu schließen und Dateien zu speichern.

- **Terminal-Server – Herunterfahren in 60 Sekunden**
  - Fährt einen Terminal-Server herunter; angemeldete Benutzer haben 60 Sekunden Zeit, um Anwendungen zu schließen und Dateien zu speichern.

Core.2 Macintosh Procedures

Core.2 Macintosh Procedures.Machine Control.Auditing

- **Sammelt Infos zu HDD, Benutzer, Prozess, Netzwerk**
  - Sammelt Informationen über einen Mac. Funktioniert auch auf fast jeder Linux-Verteilung, wenn diese unterstützt wird. Führt DF (Bereitstellungspunkt, Festplattenspeicherinformationen) uname -a (Os Information) ls /Benutzer/ (Benutzerinformationen) ifconfig (NIC-Informationen) netstat (Netzwerkverbindungsinformationen) ps aux (Prozessinformationen) aus. Ergebnisse werden an /tmp/macinfo.txt gesendet und an den Kaseya Server zurückgeleitet. Unter Audit anzeigen –> Dokumente für den Agent.
- **Liste an Disks abrufen und E-Mail an mich**
  - Verwendet DISKUTIL, um alle Mac OS X-Disks aufzulisten, ruft eine Liste von Disks aus dem Systemordner Datei abrufen ab und sendet eine E-Mail an den Administrator, der die Agent-Prozedur ausgeführt/geplant hat.

Core.2 Macintosh Procedures.Machine Control.Monitoring

- **SMART Status von Disk0 prüfen**
  - Verwendet DISKUTIL, um SMART-Status (Self-Monitoring, Analysis and Reporting Technology) von Disk0 auf dem Mac zu nutzen und sendet eine E-Mail an den Administrator, der das Verfahren ausgeführt/geplant hat, wenn der SMART-Status fehlerhaft ist.

Core.2 Macintosh Procedures.Machine Control.Networking

- **Mac mit einer Active Directory-Domäne verbinden**
  - Verwendet DSCONFIGAD, um ein Mac OS X-System an eine Active Directory-Domäne zu binden. Fragt nach vollständigem AD-Domain-Namen, AD Domain "Administrator"-Anmeldeinformationen und Ziel OU.

Core.2 Macintosh Procedures.Machine Control.System

- **Einstellungen für Mac Energiesparer konfigurieren**
  - Konfiguriert die Systemvoreinstellungen von Macintosh – Einstellungen Energiesparer Verwendet PMSET, um das Netzteilprofil zu konfigurieren (z. B. wenn der Mac an Netzbetrieb angeschlossen wird): Display-Schlaf-Modus nach 45 Minuten Inaktivität Computer-Schlaf-Modus nach 1 Stunde Inaktivität
- **Mac IP/Name Konfigurationseinträge aktualisieren.**
  - Verwendet CHANGEIP, um IP/Namensänderungen auf Mac OS X-Rechnern zu beheben. Fragt nach "Altem Namen" und "Neuem Namen"; CHANGEIP wird verwendet, um Konfigurationseinträge manuell zu aktualisieren, wenn sich die IP-Adresse oder der Hostname so geändert haben, dass betroffene Dienste nicht mehr ordnungsgemäß verarbeiten können. Beispiel: Der Server befindet sich hinter einem NAT-Dienst und die WAN-Identität hat sich geändert. Dieser Befehl wird normalerweise von einem Administrator verwendet, um betroffene Dienste zu korrigieren, wenn sich die Netzwerkinformationen eines Servers ändern. CHANGEIP kann aufgerufen werden, bevor die Änderung übernommen wird; bei einem solchen Aufruf bestehen die Argumente aus den aktuellen und noch offenen IP-Adressen, und optional aus dem vorhandenen und neuen Hostnamen.
- **Mac-Rechnernamen ändern**
  - Mac mit SCUTIL neu benennen

Core.2 Macintosh Procedures.Machine ControlSystem Preferences.Energy Saver.Battery Profile

- **Energiesparer – Akku automatisch auf Helligkeit reduzieren setzen, bevor Display-Standbymodus Aus**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren stellt ein auf "automatisch Helligkeit reduzieren, bevor Display-Standbymodus Aus".
- **Energiesparer – Akku automatisch auf Helligkeit reduzieren setzen, bevor Display-Standbymodus Ein**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren stellt ein auf "automatisch Helligkeit reduzieren, bevor Display-Standbymodus Ein".
- **Energiesparer – Akku Einstellung Computer-Standbymodus 120 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Computer-Standbymodus 120 Minuten" fest.
- **Energiesparer – Akku Einstellung Computer-Standbymodus 15 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Computer-Standbymodus 15 Minuten" fest.
- **Energiesparer – Akku Einstellung Computer-Standbymodus 30 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Computer-Standbymodus 30 Minuten" fest.
- **Energiesparer – Akku Einstellung Computer-Standbymodus 45 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Computer-Standbymodus 45 Minuten" fest.
- **Energiesparer – Akku Einstellung Computer-Standbymodus 60 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Computer-Standbymodus 60 Minuten" fest.
- **Energiesparer – Akku Einstellung Computer-Standbymodus 90 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Computer-Standbymodus 90 Minuten" fest.
- **Energiesparer – Akku Einstellung Display-Standbymodus 120 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display-Standbymodus 120 Minuten" fest.
- **Energiesparer – Akku Einstellung Display-Standbymodus 15 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display-Standbymodus 15 Minuten" fest.
- **Energiesparer – Akku Einstellung Display-Standbymodus 30 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display-Standbymodus 30 Minuten" fest.
- **Energiesparer – Akku Einstellung Display-Standbymodus 45 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display-Standbymodus 45 Minuten" fest.

- **Energiesparer – Akku Einstellung Display-Standbymodus 60 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display-Standbymodus 60 Minuten" fest.
- **Energiesparer – Akku Einstellung Display-Standbymodus 90 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display-Standbymodus 90 Minuten" fest.
- **Energiesparer – Akku Einstellung Festplatte(n) in Standbymodus Wenn Möglich Aus**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren setzt "Festplatte(n) in Standbymodus Wenn Möglich Aus".
- **Energiesparer – Akku Einstellung Festplatte(n) in Standbymodus Wenn Möglich Ein**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren setzt "Festplatte(n) in Standbymodus Wenn Möglich Ein".
- **Energiesparer – Akku Einstellung Ruhezustandsmodus 0 (Aus Speicher aktivieren)**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Ruhezustandsmodus 0 (Aus Speicher aktivieren)" fest.
- **Energiesparer – Akku Einstellung Ruhezustandsmodus 25 (Aus Disk aktivieren)**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Ruhezustandsmodus 25 (Aus Disk aktivieren)" fest.
- **Energiesparer – Akku Einstellung Ruhezustandsmodus 3 (Aus Speicher oder Disk aktivieren)**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Ruhezustandsmodus 3 (Aus Speicher oder Disk aktivieren)" fest.
- **Energiesparer – Akku Einstellung Display leicht abdunkeln Aus**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display leicht abdunkeln Aus" fest.
- **Energiesparer – Akku Einstellung Display leicht abdunkeln Ein**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Akkuprofil Verfahren legt "Display leicht abdunkeln Ein" fest.

Core.2 Macintosh Procedures.Machine Control.System Preferences.Energy Saver.Power Adapter Profile

- **Energiesparer – Netzteil Auf automatisch setzen Helligkeit reduzieren, bevor Display-Standbymodus Aus**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren stellt ein auf "automatisch Helligkeit reduzieren, bevor Display-Standbymodus Aus".
- **Energiesparer – Netzteil Auf automatisch setzen Helligkeit reduzieren, bevor Display-Standbymodus Ein**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren stellt ein auf "automatisch Helligkeit reduzieren, bevor Display-Standbymodus Ein".
- **Energiesparer – Netzteil Einstellung Computer-Standbymodus 120 Minuten**

- Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Computer-Standbymodus 120 Minuten" fest.

- **Energiesparer – Netzteil Einstellung Computer-Standbymodus 15 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Computer-Standbymodus 15 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Computer-Standbymodus 30 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Computer-Standbymodus 30 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Computer-Standbymodus 45 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Computer-Standbymodus 45 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Computer-Standbymodus 60 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Computer-Standbymodus 60 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Computer-Standbymodus 90 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Computer-Standbymodus 90 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Display-Standbymodus 120 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Display-Standbymodus 120 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Display-Standbymodus 15 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Display-Standbymodus 15 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Display-Standbymodus 30 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Display-Standbymodus 30 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Display-Standbymodus 45 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Display-Standbymodus 45 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Display-Standbymodus 60 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Display-Standbymodus 60 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Display-Standbymodus 90 Minuten**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Display-Standbymodus 90 Minuten" fest.
- **Energiesparer – Netzteil Einstellung Festplatte(n) in Standbymodus Wenn Möglich Aus**

- Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren setzt "Festplatte(n) in Standbymodus Wenn Möglich Aus".

- **Energiesparer – Netzteil Einstellung Festplatte(n) in Standbymodus Wenn Möglich Ein**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren setzt "Festplatte(n) in Standbymodus Wenn Möglich Ein".
- **Energiesparer – Netzteil Einstellung Ruhezustandsmodus 0 (Aus Speicher aktivieren)**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Ruhezustandsmodus 0 (Aus Speicher aktivieren)" fest.
- **Energiesparer – Netzteil Einstellung Ruhezustandsmodus 25 (Aus Disk aktivieren)**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Ruhezustandsmodus 25 (Aus Disk aktivieren)" fest.
- **Energiesparer – Netzteil Einstellung Ruhezustandsmodus 3 (Aus Speicher oder Disk aktivieren)**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Ruhezustandsmodus 3 (Aus Speicher oder Disk aktivieren)" fest.
- **Energiesparer – Netzwerk Einstellung Aktivieren für AirPort Netzwerkzugriff Aus**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Aktivieren für AirPort Netzwerkzugriff Aus" fest.
- **Energiesparer – Netzwerk Einstellung Aktivieren für AirPort Netzwerkzugriff Ein**
  - Verwendet PMSET, um Systemvoreinstellungen für Mac zu konfigurieren – Energiesparer-Einstellungen für Netzteilprofil Verfahren legt "Aktivieren für AirPort Netzwerkzugriff Ein" fest.

Core.2 Macintosh Procedures.Machine Control.System Preferences.Security

- **Sicherheit – Allgemeine Einstellung Automatisches Anmelden Deaktivieren**
  - Verwendet DEFAULTS, um Systemvoreinstellungen für Mac zu konfigurieren – Sicherheitseinstellungen für "Allgemein" Verfahren legt "Automatisches Anmelden Deaktivieren" fest und entfernt vorhandene automatische Anmeldekontoinformationen.

Core.2 Macintosh Procedures.Machine Control.Utils

- **OS X Dock neu starten**
  - Startet Mac Dock neu
- **Text-zu-Sprache-Nachricht an OS X senden**
  - Verwendet OSASCRIPT und SAY, um eine Nachricht wiederzugeben, die über Mac Audio eingegeben wurde (z. B. Text-zu-Sprache).
- **Kamerabild auf OS X aufnehmen**
  - Verwendet den Mac-Port "isightcapture", um mit der Kamera auf einem Mac ein Bild aufzunehmen.
- **Bildschirmaufnahme eines OS X-Desktops des aktuellen Benutzers aufzeichnen**
  - Führt eine Bildschirmaufnahme des aktuellen Mac OS X-Desktops des angemeldeten Benutzers durch. Die Bildschirmaufnahme-Datei wird in den Dokumenten-Ordner des Systems im Server abgerufen.

Core.2 Macintosh Procedures.Maintenance

- **Wöchentliche Wartung Macintosh**

- Führt eine Reihe von Routine-Wartungsaufgaben auf einem Macintosh OS X-Rechner aus.

- **Allgemeine Reinigung OS X**
  - Führt Systemreinigung durch, entfernt alte Protokolldateien, Arbeits- und Junk-Dateien, löscht Benutzer- und Systemcaches, rotiert System- und Anwendungsprotokolle, erstellt DYLD-Cache und Spotlight-Index neu.
- **OS X Disk-Volumes prüfen und reparieren**
  - Führt Diskprüfung und Reparaturen mithilfe von DISKUTIL durch.
- **OS X Disk-Berechtigungen reparieren**
  - Führt eine Disk-Reparatur und einen Berechtigungsvorgang mithilfe von DISKUTIL aus.

Core.2 Macintosh Procedures.Software Update

- **Mac-Softwareaktualisierung – Alle Aktualisierungen installieren und gegebenenfalls Benachrichtigung**
  - Mac-Softwareaktualisierung – ALLE Aktualisierungen installieren Werden neue Aktualisierungen installiert, Benachrichtigung senden. Siehe "Mac-Softwareaktualisierung – Alle Aktualisierungen installieren" unter Berichte – > Protokolle für Details. Details auch gespeichert für Agent unter Audit –> Dokumente.
- **Mac-Softwareaktualisierung – ALLE Aktualisierungen installieren und Ergebnisse abrufen/protokollieren**
  - Verwendet SOFTWAREUPDATE, um alle Mac-Softwareaktualisierungen zu installieren,
- **Mac-Softwareaktualisierung – Alle Aktualisierungen installieren und danach neu starten**
  - Verwendet SOFTWAREUPDATE, um alle Mac-Softwareaktualisierungen zu installieren und startet danach neu.
- **Mac Software-Aktualisierung – Abrufen und E-Mail-Liste von allen Aktualisierungen an mich**
  - Verwendet SOFTWAREUPDATE, um alle Mac-Software-Aktualisierungen in einer Datei aufzulisten, ruft die Datei ab und sendet die Liste per E-Mail an die E-Mail-Adresse des VSA-Benutzers, der das Verfahren ausführt/plant.
- **Mac-Softwareaktualisierung – Alle Aktualisierungen herunterladen und gegebenenfalls Benachrichtigung**
  - Verwendet SOFTWAREUPDATE, um alle Mac-Software-Aktualisierungen herunterzuladen, listet diese in einer Datei auf, ruft die Datei ab, indem eine Benachrichtigung generiert wird, wenn Benachrichtigungen verfügbar sind.
- **Mac-Softwareaktualisierung – Empfohlene Aktualisierungen herunterladen und gegebenenfalls Benachrichtigung**
  - Mac-Softwareaktualisierung – Empfohlene Aktualisierungen herunterladen Werden neue Aktualisierungen heruntergeladen, Benachrichtigung senden. Siehe "Mac-Softwareaktualisierung – Empfohlene Aktualisierungen herunterladen" unter Berichte –> Protokolle für Details. Details auch gespeichert für Agent unter Audit –> Dokumente.
- **Mac-Softwareaktualisierung – Empfohlene Aktualisierungen installieren und Ergebnisse abrufen/protokollieren**
  - Verwendet SOFTWAREUPDATE, um empfohlene Mac-Softwareaktualisierungen zu installieren,
- **Mac-Softwareaktualisierung – Ruft Liste aller Aktualisierungen ab und gegebenenfalls Benachrichtigung**
  - Mac-Softwareaktualisierung – Alle Aktualisierungen auflisten Werden neue Aktualisierungen ermittelt, Benachrichtigung senden. Siehe "Mac-Softwareaktualisierung – Alle Aktualisierungen auflisten" unter Berichte – > Protokolle für Details. Details auch gespeichert für Agent unter Audit –> Dokumente.

Core.3 Linux Procedures

Core.3 Linux Procedures.Machine Control.Audit Info

- **Aktuelle Speicherinformationen erhalten**
  - Aktuelle Speicherverfügbarkeitsinformationen abrufen.

- **Linux- und Kernel-Version herunterladen**
  - Ruft aktuelle Linux-Version (Name) und Kernel-Informationen ab

Core.3 Linux Procedures.Machine Control.DNS

- **HOSTS-Datei erstellen**
  - Dieses Verfahren erstellt eine neue Hosts-Datei mit Variablen und Informationen, die Sie bereitstellen.
- **DNS-Server bearbeiten**
  - Ihre DNS-Server bearbeiten
- **Host-Namen festlegen**
  - Mit diesem Verfahren wird Ihr Host-Name des Servers/Arbeitplatzrechners festgelegt.

Core.3 Linux Procedures.Machine Control.Files/Folder Control

- **Datei-/Ordner-Berechtigungen ändern**
  - Lesen – Schreiben – Ausführen 4 2 1
- **Gruppenbesitz ändern**
  - chgrp groupName folderName
- **Besitz ändern**
  - chown userName fileFolderName
- **Datei oder Ordner löschen – Gefährlich**
  - Dieses Verfahren löscht beliebige Dateien oder Ordner, ohne Erlaubnis einzuholen.

Core.3 Linux Procedures.Machine Control.Linux Kernel

- **Ein initrd-Abbild erstellen**
  - Erstellt ein initrd-Abbild des Linux-Systems und bezeichnet es als initrd.image-#version#, basierend auf einem Versionswert, den Sie eingeben.

Core.3 Linux Procedures.Machine Control.Monitoring

- **SNMP-Konfigurationsdatei herunterladen**
  - SNMP-Konfigurationsdatei mithilfe von "Datei abrufen" abrufen

Core.3 Linux Procedures.Machine Control.Networking

- **Einrichtung DHCP-Client**
  - Fügt Einträge für Schnittstelle hinzu, um DHCP-Server auszuwählen
- **Einrichtung Netzwerk (1 Schnittstelle)**
  - Dies erstellt eine neue Schnittstellen-Datei in /etc/networking mit neuen IP-Adressen-Informationen. Dies richtet nur ein Netzwerk für die 1 zentrale Schnittstelle ein. Der Netzwerk-Service wird neu gestartet, nachdem die Datei erstellt wurde.

Core.3 Linux Procedures.Machine Control.Networking.Get DOMAIN info

- **Alle Domaininformationen abfragen**
  - Führt eine vollständige DNS-Suche eines Domain-Namens durch, den Sie mithilfe von DIG mit dem ANY (zusammenstellend – Alle Domäneninformationen)-Schalter angeben und ruft die erstellte Protokolldatei, dig-#domain#-all.log, im Systemordner "GetFile" ab.
- **DNS-Server für Domain-Details abfragen**
  - Führt eine DNS-Suche eines Domain-Namens durch, den Sie mithilfe von DIG angeben und ruft die erstellte Protokolldatei, dig-#domain#.log, im Systemordner "GetFile" ab.
- **DNS-Server autoritativ für eine Domain abfragen**

- ➢ Führt eine autoritative Namenserver-Suche eines Domain-Namens durch, den Sie mithilfe von DIG mit dem NS (autoritative DNS-Server für Domain)-Schalter angeben und ruft die erstellte Protokolldatei, dig-#domain#-Auth.log, im Systemordner "GetFile" ab.

- **Domain-Adressen-Aufzeichnungen abfragen**
  - ➢ Führt eine Adressen-(A)-Datensätze DNS-Suche eines Domain-Namens durch, den Sie mithilfe von DIG mit dem NS (autoritativer DNS-Server für Domain)-Schalter angeben und ruft die erstellte Protokolldatei, dig-#domain#-A.log, im Systemordner "GetFile" ab.
- **Domain-E-Mail-Server abfragen**
  - ➢ Führt eine E-Mail-Server/Mail Exchanger (MX)-Datensätze DNS-Suche eines Domain-Namens durch, den Sie mithilfe von DIG mit dem MX (Mail Exchanger für Domain) Schalter angeben und ruft die erstellte Protokolldatei, dig-#domain#-MX.log, im Systemordner "GetFile" ab.
- **Statistiken einschließlich Roundtripzeit abfragen**
  - ➢ Führt eine DNS-Statistik-Abfrage (einschließlich Roundtripzeit) eines Domain-Namens durch, den Sie mithilfe von DIG angeben und ruft die erstellte Protokolldatei, dig-#domain#-stats.log, im Systemordner "GetFile" ab.
- **TTL für jeden Ressourcen-Datensatz abfragen**
  - ➢ Führt eine DNS-Gültigkeitsdauer (TLL)-Abfrage eines Domain-Namens durch, den Sie mithilfe von DIG angeben und ruft die erstellte Protokolldatei, dig-#domain#-TTL.log, im Systemordner "GetFile" ab.

Core.3 Linux Procedures.Machine Control.Networking.Routing

- **Routen abrufen**
  - ➢ Ruft aktuelle Routen-Einrichtung ab
- **Pfad zu Domain/IP verfolgen**
  - ➢ HOPS zu Domain/IP-Adresse verfolgen – Verwendet "Datei abrufen", um Ergebnisse anzuzeigen

Core.3 Linux Procedures.Machine Control.Reboot/Shutdown

- **Linux neu starten**
  - ➢ Startet das System neu
- **Linux herunterfahren**
  - ➢ Das Linux-System herunterfahren

Core.3 Linux Procedures.Machine Control.Runlevel Control

- **Benutzerdefinierte Ausführungsebene**
  - ➢ Erklärung zu Ausführungsebenen in Linux unter http://http://en.wikipedia.org/wiki/Runlevel
- **Ausführungsebene 1**
  - ➢ Ausführungsebene 1 ist üblicherweise für sehr einfache Befehle. Dies ist das Äquivalent zu "Abgesicherter Modus", der von Windows verwendet wird. Diese Ebene wird üblicherweise nur verwendet, um Reparaturen oder Wartungsarbeiten am System zu bewerten. Dies ist ein Einzelbenutzermodus; andere Benutzer können sich nicht am Rechner anmelden.
- **Ausführungsebene 2**
  - ➢ Ausführungsebene 2 wird verwendet, um die meisten Rechner-Dienste zu starten. Dadurch wird jedoch der Netzwerkdienst Dateifreigabe (SMB, NFS) gestartet. Dadurch können sich mehrere Benutzer am Rechner anmelden.
- **Ausführungsebene 3**
  - ➢ Ausführungsebene 3 wird häufig von Servern verwendet. Dies lädt alle Dienste außer X Windows System. Dies bedeutet, dass das System auf das Äquivalent von DOS

hochgefahren wird. Es starten keine GUIs (KDE, Gnome). Über diese Ebene können sich mehrere Benutzer am Rechner anmelden.

- **Ausführungsebene 4**
  - Ausführungsebene 4 ist üblicherweise eine benutzerdefinierte Ebene. Standardmäßig startet sie mehr Dienste als Ebene 3. Diese Ebene wird üblicherweise nur unter besonderen Umständen verwendet.
- **Ausführungsebene 5**
  - Ausführungsebene 5 umfasst alles. Dadurch werden GUIs gestartet, Extra-Dienste für Drucken und Dienste von Drittanbietern. Umfassender Support für viele Benutzer. Diese Ausführungsebene wird im Allgemeinen von Arbeitsplatzrechnern verwendet.

Core.3 Linux Procedures.Machine Control.Services Control

- **Benutzerdefinierte Dienststeuerung**
  - Start, Stopp und Neustart von beliebigen Diensten im System
- **HTTPD/Apache2 neu starten**
  - Startet Ihren Web-Dienst HTTPD/Apache2 neu
- **Netzwerk neu starten**
  - Startet den Netzwerk-Daemon neu
- **NFS neu starten**
  - Startet den NFS-Daemon-Dienst neu
- **Postfix neu starten**
  - Startet Postfix-E-Mail-Server neu
- **SSH neu starten**
  - SSH-Server neu starten
- **VMWare-Werkzeuge neu starten**
  - Startet VMWare-Werkzeuge neu

Core.3 Linux Procedures.Machine Control.User/Group Control.Groups

- **Neue Gruppe erstellen**
  - Verwendet GROUPADD, um eine neue Gruppe zu erstellen, die Sie angeben.
- **Gruppe löschen**
  - Verwendet GROUPDEL, um eine vorhandene Gruppe zu löschen, die Sie angeben.

Core.3 Linux Procedures.Machine Control.User/Group Control.Password Control

- **Stammkennwort ändern**
  - Ändert das Stammkennwort im System. Aus einem unerfindlichen Grund gibt das Skript den Status "Fehlgeschlagen" zurück, aber funktioniert weiterhin.
- **Benutzerkennwort ändern**
  - Nach Benutzername fragen und zurücksetzen

Core.3 Linux Procedures.Machine Control.User/Group Control.Users

- **Neuen Benutzer hinzufügen**
  - Neuen Linux-Benutzer hinzufügen
- **Benutzer löschen**
  - Benutzer von Server/Rechner löschen

Core.3 Linux Procedures.Machine Control.Utils

- **Benutzerdefinierte Befehle hinzufügen**

- Fügt eine Anzahl von benutzerdefinierten Befehlen mit Alias zur /root/.bashrc-Datei hinzu und führt sie dann aus, damit diese Befehle wirksam werden. Die benutzerdefinierten Befehle sind:
  ll = ls –l
  la = ls -A
  l = ls -CF
  *** Durch Hinzufügen weiterer Befehle mit Alias erweitern ***

- **Systemuhr synchronisieren**
  - Installiert und synchronisiert die Uhr.
- **Dateidatenbank aktualisieren**
  - Aktualisiert die Datenbank des Dateisystems zur Verwendung des Befehls "Lokalisieren".

Core.3 Linux Procedures.Maintenance

- **I-Knoten-Benutzerstatistiken erfassen**
  - Prüft I-Knoten-Nutzung.
- **Logische Dateisystemüberprüfung (FSCK) beim nächsten Neustart erzwingen**
  - Erzwingt, dass beim nächsten Neustart eine Dateisystemüberprüfung (File System Check, FSCK) durchgeführt wird.
- **Datenträgernutzung abrufen**
  - Erzeugt eine Liste der Datenträgernutzung mit DF, schreibt die Ergebnisse in das Skripting-Protokoll und ruft die Ergebnisse in den Ordner "Get File" des Systems ab.
- **Wöchentliche Linux-Wartung**
  - Führt eine Reihe von Routine-Wartungsaufgaben bei Linux-Rechnern durch, einschließlich Zeitsynchronisierung, "apt-get" Repository-Bereinigung, Paket-Upgrades/Aktualisierungen sowie Datenträgerüberprüfungen und Leistungsstatistiken.
- **Permanente Adobe Flash/Macromedia-Benutzerobjekte entfernen**
  - Entfernt permanente Adobe Flash/Macromedia-Benutzerobjekte.
- **Temporäre Benutzerdateien entfernen**
  - Entfernt temporäre Dateien (d. h. *~) aus dem Basisordner des aktuellen Benutzers.

Core.3 Linux Procedures.Process Control.Get All Processes with PID

- Ruft alle Prozesse mit Prozess-ID ab, ruft die Ergebnisse mit der Funktion "GET FILE" ab.

- **Prozessstruktur abrufen**
  - Erzeugt eine STRUKTUR von über- und untergeordneten Prozessen; ruft die Ergebnisse mit der Funktion "GET FILE" ab.
- **Prozess entfernen**
  - Die Variable mit der richtigen PID wird zum Entfernen des Gliederungsprozesses verwendet.
- **Eine Datei lokalisieren**
  - Verwendet die Lokalisierungsfunktion in Kaseya, um nach Dateien wie angegeben zu suchen und verwendet die Funktion "GET FILE", um die Ergebnisse abzurufen.

Core.3 Linux Procedures.Setup/Configs.Backup Servers

- **MySQL Backups With AutoMySQLBackup On Ubuntu 9.10**
  - Postfix-Installation vor Installation von AutoMySQLBackup erforderlich – Postfix ist erforderlich http://sourceforge.net/projects/automysqlbackup/ http://www.mysql.com/
- **Ubuntu Server 9.04 Bacula Bweb GUI**
  - Nicht getestet----

Core.3 Linux Procedures.Setup/Configs.CRM Servers.SugarCRM

- Vollständige Installation von LAMP-Server vor Installation von SugarCRM erforderlich – MySQL, Apached, PHP – Wenn das Skript abgeschlossen wurde, führen Sie Folgendes aus: http://Server-IP-Adresse/sugarcrm

Core.3 Linux Procedures.Setup/Configs.DNS

- **DNS-Server mit chroot einrichten**
  - Konfiguriert BIND zur Ausführung in einer Umgebung mit chroot.

Core.3 Linux Procedures.Setup/Configs.Email Server

- **(2) Postfix-E-Mail-Server konfigurieren**
  - Konfiguriert den Postfix-E-Mail-Server
- **(2.1) SMTP-AUTH konfigurieren**
  - Konfiguriert sichere SMTP-Authentifizierung mit SASLAUTHD
- **(3) Zertifikate für TLS erstellen**
  - Erstellt TLS-Zertifikate
- **(4) Postfix für TLS konfigurieren**
  - Konfiguriert TLS-Sicherheitsschlüssel zur Verwendung von Postfix
- **(5) SASLAUTHD zur Arbeit mit Postfix mit chroot konfigurieren**
  - Die Authentifizierung geschieht durch SASLAUTHD. Sie müssen einige Elemente ändern, damit es korrekt funktioniert. Da Postfix mit chroot in /var/spool/postfix ausgeführt wird, ist wie folgt vorzugehen:
- **(6) Courier-IMAP/Courier-POP3 installieren**
  - Installieren und konfigurieren Sie IMAP und POP3 mit courier-... und ändern Sie die folgenden zwei Dateien: ersetzen Sie CN=localhost durch CN=server1.beispiel.com (Sie können bei Bedarf auch die anderen Werte ändern): vim /etc/courier/imapd.cnf vim /etc/courier/pop3d.cnf
- **(7) Maildir konfigurieren**
  - Konfiguriert Maildir für E-Mail-Nachrichten und Benutzerpostfächer

Core.3 Linux Procedures.Setup/Configs.FTP Servers

- **Proftpf konfigurieren**
  - Konfiguriert den Proftpd-Server – Denken Sie daran, die Software zuerst zu installieren.

Core.3 Linux Procedures.Setup/Configs.MySQL Server

- **Installation von MySQL-Server**
  - Installieren Sie MySQL-Server und richten Sie ein Stammkennwort ein

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Client

- **NFS-Client installieren und konfigurieren**
  - NFS-Einrichtung für Client-Rechner, um Laufwerke als vom Server exportiert/freigegeben bereitzustellen

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Server

- **NFS-Server installieren und einrichten**
  - Installiert und konfiguriert den NFS-Server mit dem Basisverzeichnis und einem optionalen, für Clients freigegebenen Verzeichnis.

Core.3 Linux Procedures.Setup/Configs.Security.AppArmor

- **AppArmor deaktivieren**

- AppArmor ist eine Sicherheitserweiterung (vergleichbar mit SELinux), die erweiterte Sicherheit bietet. Meiner Meinung nach müssen Sie kein Sicherheitssystem konfigurieren, es bringt in der Regel mehr Probleme als Vorteile mit sich (wenn Sie eine Woche lang auf Fehlersuche waren, weil ein Dienst nicht wie erwartet funktionierte und Sie dann herausfinden, dass alles in Ordnung war, war AppArmor die Ursache des Problems). Darum deaktiviere ich es.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Forward Rules

- **Zugriff auf ein bestimmtes Subnetz verweigern**
  - Verweigert den Zugriff auf ein Subnetz, das Sie durch Hinzufügen der angemessenen Firewall-Regeln für iptables angeben.
- **Datenverkehr weiterleiten (DNAT)**
  - Ermöglicht die DNAT-Weiterleitung eines bestimmten TCP-Ports zum internen Server. Sie können die öffentliche Schnittstelle, öffentliche Adresse, interne Serveradresse und den Port angeben und das Verfahren fügt die entsprechenden Firewall-Regeln für iptables hinzu.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Global Rules (REJECT, ACCEPT)

- **# Forwarding Traffic (DROP ALL)**
  - Lehnt sämtlichen Datenverkehr aus der Weiterleitungskette ab
- **# Incoming Traffic (ALLOW ALL)**
  - Erlaubt sämtlichen eingehenden Datenverkehr durch die INPUT-Kette
- **# Incoming Traffic (DROP ALL)**
  - LEHNT sämtlichen eingehenden Datenverkehr ab
- **# Outgoing Traffic (ALLOW ALL)**
  - Erlaubt sämtlichen Datenverkehr, der Ihr internes Netzwerk verlässt
- **# Outgoing Traffic (DROP ALL)**
  - Verweigert dem internen Datenverkehr den Austritt aus der Firewall
- **_### NB! - Routing aktivieren - NB! ###_**
  - Routing und NAT für iptables aktivieren – Wichtig für die Verarbeitung von Datenverkehr durch die Firewall
- **ICMP-Umleitungsmeldungen nicht akzeptieren**
  - Konfiguriert das System so, dass keine ICMP-Umleitungen akzeptiert werden.
- **ICMP-Umleitungsmeldungen nicht senden**
  - Konfiguriert das System so, dass keine ICMP-Umleitungen gesendet werden.
- **An Broadcast- oder Multicast-Adressen gesendete ICMP-Echoanforderungsmeldungen verwerfen**
  - Konfiguriert das System so, dass es ICMP-Echoanforderungsmeldungen, die an Broadcast- oder Multicast-Adressen gesendet wurden, verwirft.
- **An Quelle geleitete Pakete verwerfen**
  - Konfiguriert das System so, dass es an die Quelle geleitete Pakete verwirft.
- **Protokollierung aktivieren**
  - Aktiviert die Firewall-Ereignisprotokollierung von iptables.
- **Spoofing-Schutz der Quelladresse aktivieren**
  - Aktiviert Spoofing-Schutz der Quelladresse im System.
- **TCP-SYN-Cookie-Schutz vor SYN-Flutangriffen aktivieren**
  - Aktiviert TCP-SYN-Cookie-Schutz vor SYN-Flutangriffen im System.
- **Alle Ketten leeren**

  - Leert alle iptables-Regeln – Vorsicht, wird auf eigenes Risiko hin verwendet!
- **Pakete mit unmöglichen Quelladressen protokollieren**
  - Aktiviert die Protokollierung von Paketen mit unmöglichen Quelladressen im System.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Inbound Rules

- **Eingang von CUSTOM-Port erlauben**
  - Erlaubt Ihnen die Eingabe eines Schnittstellenprotokolls und eines TCP/UDP-Ports, den Sie den Firewall-Regeln für iptables hinzufügen möchten.
- **DNS-Eingang erlauben**
  - Erlaubt eingehenden DNS-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables. Gilt nicht nur für Firewalls, die als DNS-Clients wirken, sondern auch für Firewalls in der Rolle eines zwischenspeichernden oder normalen DNS-Servers.
- **FTP-Eingang erlauben**
  - Erlaubt eingehenden FTP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **ICMP-Eingang erlauben**
  - Erlaubt eingehenden ICMP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables. iptables ist so konfiguriert, dass die Firewall ICMP-Echoanforderungen (Pings) senden und im Gegenzug die erwarteten ICMP-Echoantworten akzeptieren darf.
- **IMAP-Eingang erlauben**
  - Erlaubt eingehenden IMAP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **IMAPS-Eingang erlauben**
  - Erlaubt eingehenden IMAPS-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Kaseya-Eingang erlauben**
  - Erlaubt eingehenden Kaseya-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Loopback-Schnittstelle erlauben**
  - Erlaubt eingehenden Loopback-Schnittstellen-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **MySQL erlauben**
  - Erlaubt eingehenden MySQL-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Netzwerk Zugriff auf Firewall erlauben**
  - eth1 ist direkt mit einem privaten Netzwerk mit IP-Adressen aus dem 192.168.1.0-Netzwerk verbunden. Für sämtlichen Datenverkehr zwischen diesem Netzwerk und der Firewall wird vereinfachend angenommen, dass er vertrauenswürdig und erlaubt ist. Für die mit dem Internet verbundene Schnittstelle sind weitere Regeln notwendig, um nur bestimmten Ports, Verbindungstypen und eventuell sogar bestimmten Remote-Servern den Zugriff auf Ihre Firewall und Ihr Heimnetzwerk zu gestatten.
- **POP3-Eingang erlauben**
  - Erlaubt eingehenden POP3-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **POP3S-Eingang erlauben**
  - Erlaubt eingehenden POP3S-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **SMTP-Eingang erlauben**

- ➢ Erlaubt eingehenden SMTP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **SSH-Eingang erlauben**
  - ➢ Erlaubt eingehenden SSH-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Datenverkehr von Localhost erlauben**
  - ➢ Erlaubt eingehenden Datenverkehr von der Localhost-Adresse durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **WWW-Eingang erlauben**
  - ➢ Eingehende Pakete für Port 80 und 22 sind erlaubt, sodass der erste Schritt zum Verbindungsaufbau erfolgt. Diese Ports müssen nicht für das Rückkehrprotokoll angegeben werden, da ausgehende Pakete für alle bestehenden Verbindungen erlaubt sind. Verbindungen, die von auf dem Webserver angemeldeten Personen initiiert wurden, werden abgelehnt, da ausgehende NEUE Verbindungspakete nicht erlaubt sind.
- **Eingang von bestehenden Sitzungen erlauben**
  - ➢ Erlaubt eingehenden Datenverkehr von bestehenden Verbindungen durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **IP-Adresse blockieren**
  - ➢ Verhindert, dass eine von Ihnen angegebene IP-Adresse in Ihr Netzwerk über die öffentliche Schnittstelle eintritt.
- **IRC-Eingang blockieren**
  - ➢ Blockiert eingehenden IRC-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Netzwerk blockieren**
  - ➢ Blockiert den Zugriff eines ganzen Netzwerks auf Ihr Netzwerk.
- **Alle iptables-Regeln auflisten**
  - ➢ Dadurch werden alle iptables-Regeln zu /var/tmp/iptables.log weitergereicht und das GET-Verfahren lädt dies zur Überprüfung auf den Server hoch.
- **IPTables neu starten**
  - ➢ Startet IPTables-Firewall neu
- **iptables-Regeln speichern**
  - ➢ Auf Ubuntu getestet

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Outbound Rules

- **# Allow Kaseya Outbound**
  - ➢ Erlaubt ausgehenden Kaseya-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Ausgang von CUSTOM-Port erlauben**
  - ➢ Erlaubt einem benutzerdefinierten Port Ihres internen Netzwerks den Zugriff auf die Außenwelt.
- **DNS-Ausgang erlauben**
  - ➢ Die folgenden Anweisungen gelten nicht nur für Firewalls, die als DNS-Clients wirken, sondern auch für Firewalls in der Rolle eines zwischenspeichernden oder normalen DNS-Servers.
- **Ausgang von bestehenden Verbindungen erlauben**
  - ➢ Erlaubt alle bestehenden Verbindungen mit ACK-Rückleitung.
- **FTP-Ausgang erlauben**

- Erlaubt ausgehenden FTP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.

- **Ausgehende ICMP-Pakete erlauben**
  - Erlaubt ausgehende ICMP-Pakete durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **IMAP-Ausgang erlauben**
  - Erlaubt ausgehenden IMAP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **IMAPS-Ausgang erlauben**
  - Erlaubt ausgehenden IMAPS-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Loopback-Schnittstelle erlauben**
  - Erlaubt ausgehenden Loopback-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **MySQL-Ausgang erlauben**
  - Erlaubt ausgehenden MySQL-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **POP3-Ausgang erlauben**
  - Erlaubt ausgehenden POP3-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **POP3S-Ausgang erlauben**
  - Erlaubt ausgehenden POP3S-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **SMTP-Ausgang erlauben**
  - Erlaubt ausgehenden SMTP-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **SSH erlauben**
  - Erlaubt ausgehenden SSH-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **WWW erlauben**
  - Erlaubt ausgehenden WWW-Datenverkehr durch Hinzufügen der angemessenen Firewall-Regeln für iptables.
- **Zugriff auf eine bestimmte ausgehende IP-Adresse mit Protokollierung verweigern**
  - Verweigert den Zugriff mit Protokollierung auf eine ausgehende IP-Adresse, die Sie durch Hinzufügen der angemessenen Firewall-Regeln für iptables angeben.
- **OUTBOUND-Regeln LEEREN**
  - Leert OUTBOUND-Regeln von iptables. Vorsicht, wird auf eigenes Risiko hin verwendet!
- **Alle OUTBOUND-Regeln ausführen**
  - Wendet alle OUTBOUND-Regeln an mit der Möglichkeit, optional alle OUTBOUND-Regeln zuerst zu leeren.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Postrouting Rules

- **Routing für privates Netzwerk durch Firewall erlauben**
  - Sie werden feststellen, dass das private Netzwerk ein weitergeleitetes nicht-öffentliches IP-Netzwerk ist. Darum ist eine Adressenübersetzung an einem Router mit öffentlicher IP-Adresse notwendig, anderenfalls kann kein Element im öffentlichen Netzwerk Pakete an das private Netzwerk zurückgeben. Die Adressenübersetzung wird mit iptables einfach aktiviert. Die zu übersetzenden Adressen sind die "Quelle" (Source) für Sitzungen, darum wird der Modus als "Source NAT (SNAT)" bezeichnet:

Core.3 Linux Procedures.Setup/Configs.Security.SELinux

- **SELinux nach Neustart deaktivieren**
  - Dadurch wird SELinux nach dem ersten Neustart ordnungsgemäß deaktiviert.
- **SELinux sofort deaktivieren**
  - Deaktiviert SELinux für die aktuell angemeldete Ausführungsebene. Dies ist nicht so konfiguriert, dass es nach einem Neustart deaktiviert wird.

Core.3 Linux Procedures.Setup/Configs.Shell Control

- **Standard-Shell ändern**
  - /bin/sh ist eine symbolische Verknüpfung zu /bin/dash, Sie benötigen jedoch /bin/bash, nicht /bin/dash.

Core.3 Linux Procedures.Setup/Configs.Web Servers.Apache2

- **Module aktivieren**
  - Apache-Module (SSL, rewrite, suexec, include und WebDAV)
- **Apache2 installieren**
  - Verwendet APT-GET zur Installation des Apache2-Webservers, CHKCONFIG zur Einstellung des automatischen Starts und startet den Apache-Daemon.
- **PHPMyAdmin installieren**
  - Vergewissern Sie sich, dass Sie die Apache-Konfiguration geändert haben, sodass phpMyAdmin nicht nur Verbindungen von Localhost erlaubt (durch Kommentieren der Stanza von <Verzeichnis /usr/share/phpMyAdmin/>):

Core.3 Linux Procedures.Setup/Configs.Web Servers.Scripting

- **PHP5 installieren**
  - Installiert PHP5 für Apache 2.

Core.3 Linux Procedures.Software Control.Applications

- **CHKCONFIG installieren**
  - Installiert das CHKCONFIG-Paket. Mit diesem Paket können Sie ein bestimmtes Daemon-Paket beim Systemstart starten.
- **CHKCONFIG einfach installieren**
  - Verwendet APT-GET zur Installation von CHKCONFIG.
- **Häufig verwendete Pakete installieren**
  - Installiert Pakete für Ubuntu, die für gewöhnlich notwendig sind. binutils cpp fetchmail flex gcc libarchive-zip-perl libc6-dev libcompress-zlib-perl libdb4.6-dev libpcre3 libpopt-dev lynx m4 make ncftp nmap openssl perl perl-modules unzip zip zlib1g-dev autoconf automake1.9 libtool bison autotools-dev g++ build-essential
- **SNMP installieren**
  - Installiert SNMP, mit dem Sie Linux-Server überwachen können. Denken Sie daran, Ihren SNMP-Community-String einzurichten.
- **Software installieren**
  - Fragt den Benutzer nach dem Namen des zu installierenden Softwarepakets und installiert dieses Paket dann mit APT-GET.
- **Software aus Abbildliste installieren**
  - Ermöglicht Ihnen, eine Liste von Software mit einem senkrechten Strich (|) zum APT-GET-Installationsbefehl zu versehen, mit dem sämtliche fehlende Software aus der Liste installiert wird. Sie müssen zuerst die Liste erstellen. NB (für das Verfahren zur Erstellung der Abbildliste siehe Ordner für Softwareaktualisierungen/Upgrades)

- **SSH installieren**
  - Installiert den SSH-Server für Remotezugriff.
- **VIM installieren**
  - Installiert VIM, einen leicht zu bedienenden Editor für Textdateien in Linux.
- **vim-nox installieren**
  - Das vi-Standardprogramm legt ein merkwürdiges Verhalten in Ubuntu und Debian an den Tag; installieren Sie vim-nox, um dieses Problem zu beheben:
- **XPDF installieren**
  - PDF-Reader für Linux

Core.3 Linux Procedures.Software Control.apt-get

- **apt-get automatisch bereinigen**
  - apt-get autoclean entfernt nur Paketdateien, die nicht mehr heruntergeladen werden können.
- **apt-get Repository löschen**
  - Entfernt alles außer gesperrte Dateien aus /var/cache/apt/archives/ und /var/cache/apt/archives/partial/. Wenn Sie also ein Paket neu installieren müssen, sollte APT es wieder abrufen.
- **Software installieren**
  - Fragt den Benutzer nach dem Namen des zu installierenden Softwarepakets und installiert dieses Paket dann mit APT-GET.
- **Software entfernen**
  - Entfernt das Paket wie vom Verfahren aufgefordert.

Core.3 Linux Procedures.Software Control.DNS

- **Bind9 installieren**
  - DNS-Server für Linux

Core.3 Linux Procedures.Software Control.Email Servers

- **Zimbra E-Mail herunterladen**
  - Lädt die Zimbra E-Mail Collaboration Suite für Linux herunter.

Core.3 Linux Procedures.Software Control.File Server

- **Quota installieren**
  - Installiert die Quota-Anwendung, die für die Quota-Steuerung bestimmter Ordner notwendig ist. Es wird empfohlen, dass Sie die Datei /etc/fstab manuell bearbeiten, da dadurch Ihr Server beschädigt werden kann und kein Dateisystem bereitzustellen. Hier ist ein Beispiel eines funktionierenden fstab mit aktiviertem Quota:

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    nodev,noexec,nosuid 0       0
/dev/mapper/server1-root /               ext4
errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0
1
# /boot was on /dev/sda1 during installation
UUID=a8f37dcf-5836-485c-a451-3ae2f0f47720 /boot          ext2    defaults
0       2
/dev/mapper/server1-swap_1 none            swap    sw              0       0
/dev/fd0        /media/floppy0  auto    rw,user,noauto,exec,utf8 0       0
```

- **Quota einschalten**
  - Aktiviert Quota-Verwaltung für Dateiserver

Core.3 Linux Procedures.Software Control.FTP Servers

- **Proftpd installieren**
  - Installiert den Proftp-Server für Linux

Core.3 Linux Procedures.Software Control.iptables (Firewall)

- **iptables installieren**
  - Verwendet APT-GET zur Installation einer iptables-Firewall.

Core.3 Linux Procedures.Software Control.Management Software

- **Webmin herunterladen**
  - Webmin ist eine GUI, die zur vollständigen Verwaltung von Linux mit Ihrem Webbrowser verwendet wird.

Core.3 Linux Procedures.Software Control.Repository's

- **Multiverse-Repository aktivieren**
  - Dadurch werden die Quellen zur source.list-Datei hinzugefügt. Es erstellt nicht die Datei neu.
- **Universe-Repository aktivieren**
  - Dieses Verfahren fügt diese Repositorys zur Quelldatei hinzu. Es erstellt nicht die Datei neu.
- **Repositorys aktualisieren**
  - Aktualisiert alle Pakete – Führen Sie dies nach Hinzufügen der Repositorys aus.

Core.3 Linux Procedures.Software Control.System

- **NTP-Daemon installieren**
  - Es hat sich bewährt, die Systemuhr mit einem NTP (Network Time Protocol)-Server über das Internet zu synchronisieren. Einfach ausführen

Core.3 Linux Procedures.Software Control.Updates/Upgrades

- **Abbildliste der installierten Software erstellen**
  - Erstellt eine Abbildliste der installierten Software
- **Vollständige Systemaktualisierung**
  - Aktualisiert alle Systempakete
- **Upgrade von Paketen durchführen**
  - Mit diesem Verfahren führen Sie ein Upgrade von Paketen innerhalb derselben Distribution durch.
- **Upgrade auf neue Version**
  - Führt ein Upgrade Ihrer Linux-Distribution auf die neueste verfügbare Version durch. Nach Abschluss wird Ihnen eine Neustartanfrage auf dem Desktop angezeigt.
- **Aktualisierungen/Upgrades von Linux-Paketen**
  - Führt eine vollständige Systemaktualisierung und ein Upgrade aller installierten Pakete durch.

Core.4 Verfahren für andere Tools und Dienstprogramme

Core.4 Other Tools and Utility Procedures.AntiVirus

- **EICAR-Virustest**
  - Erstellt eine Datei im Agent-Arbeitsverzeichnis, die das Muster des EICAR-Testvirus enthält. Diese Agent-Prozedur kann verwendet werden, um zu prüfen, ob auf einem Rechner

Antivirensoftware ausgeführt wird. HINWEIS: Dabei handelt sich um keinen echten Virus und es besteht kein Risiko. Weitere Informationen erhalten Sie unter http://eicar.org.

- **Vollständigen Scan mit Tool zum Entfernen bösartiger Software ausführen und bereinigen**
  - Verwendet das Microsoft Tool zum Entfernen bösartiger Software, um einen vollständigen Scan und eine Bereinigung durchzuführen. Ergebnisse des Vorgangs werden in einer MRT.LOG-Datei und im Skripting-Protokoll protokolliert. Die Protokolldatei wird in den Ordner "GetFile" des Systems abgerufen.

Core.4 Other Tools and Utility Procedures.AntiVirus.Defender

- **Windows Defender - Vollständiger Systemscan**
  - Führt einen vollständigen Systemscan mit Windows Defender aus.
- **Windows Defender - Schneller Systemscan**
  - Führt einen schnellen Systemscan mit Windows Defender aus.
- **Windows Defender - Signaturaktualisierung**
  - Führt eine Signaturaktualisierung von Windows Defender aus.

Core.4 Other Tools and Utility Procedures.AutoAdminLogon

- **AutoAdminLogon deaktivieren**
  - Deaktiviert alle vorher aktivierten AutoAdminLogon-Konfigurationen auf einem Windows-Rechner.
- **AutoAdminLogon mit AUTOLOGON aktivieren**
  - Aktiviert AutoAdminLogon mit sicherer Kennwortverschlüsselung durch das Dienstprogramm SysInternals AutoLogon. Diese Agent-Prozedur funktioniert nur auf 32-Bit-Versionen von Windows XP oder höher.
- **AutoAdminLogon mit Klartextmethode aktivieren**
  - Fragt nach Benutzernamen und Kennwort, die bei AutoAdminLogin verwendet werden sollen und aktiviert dann die AutoAdminLogin-Konfiguration in Klartext auf einem Windows-Rechner mithilfe der angegebenen Anmeldedaten.

Core.4 Other Tools and Utility Procedures.Kaseya Agent Management

- **Agent – Einchecken erzwingen**
  - Dies ist das absolut kürzeste Verfahren. Bei diesem Verfahren gibt es keine Schritte. Es soll den Agent einfach zum Einchecken auf dem KServer zwingen. Ermitteln Sie mithilfe von 'Einchecken erzwingen', ob ein Agent online ist.
- **Agent – Kaseya aus Startmenü entfernen und Programme hinzufügen/entfernen**
  - Agent-Ordner aus Startmenü entfernen Blenden Sie das Symbol in der Systemablage aus (blaues K), indem Sie das Agent-Menü deaktivieren (Registerkarte 'Agent' - Menü 'Agent'). Führen Sie dieses Skript auf Rechnern aus, auf denen niemand den Agent deinstallieren, beenden oder stoppen soll.
- **Agent – Audit-Cache zurücksetzen**
  - Die vom Agent gespeicherte, gecachte Datei mit dem Inventarisierungsergebnis wird gelöscht. Führen Sie dieses Verfahren aus, um alle Anwendungsergebnisse aus einer Inventarisierung zurückzusetzen und erneut zu beginnen.
- **Agent – Remote-Control-Sitzungen beenden**
  - Dieses Skript beendet alle Remote-Control-Sitzungen, die Kaseya in der Remote-Control-Funktion von VSA (K-VNC, WinVNC, Terminaldienste, FTP, RAdmin und pcAnyWhere) unterstützt.
- **VNC – Taskleistensymbol ausblenden**
  - Deaktiviert das VNC-Taskleistensymbol bei Windows-Rechnern, wenn der VNC-Dienst ausgeführt wird.

- **VNC – Zeitlimit für Leerlauf auf 0 setzen (kein Zeitlimit)**
  - Stellt das VNC-Zeitlimit für Leerlauf auf 0, sodass bei einer VNC-RC-Sitzung die Verbindung nicht getrennt wird. Nützlich beim Durchführen von Remote-Vorgängen auf Rechnern, die viel Zeit zum Abschluss brauchen und bei denen es bei einer VNC-Sitzung nicht automatisch nach einer Stunde Inaktivität (Standardeinstellung) zu einer Zeitüberschreitung kommt.
- **VNC – Hintergrund bei Fernsteuerung aktivieren**
  - Aktiviert Hintergrund, wenn ein Systempaar ferngesteuert wird, wobei das VNC-Symbol zur vollständig automatischen Fernsteuerung eines Agent deaktiviert wird
- **VNC – RealVNC aus Startmenü entfernen**
  - Entfernt den RealVNC-Eintrag aus dem Startmenü.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Ping Check

- **Ping IP-Adresse1**
  - Dieses Verfahren ruft per 'Ping' eine IP-Adresse auf, um Ergebnisse zu erhalten, die Sie in einem anderen Verfahren verwenden können. Dies könnte auch ein Port oder ein anderes Gerät sein.
- **Ping IP-Adresse2**
  - Dieses Verfahren testet die Variable der Ping-IP-Adresse, um zu untersuchen, ob die Adresse per Ping aufgerufen werden kann, ohne dass ein Paketverlust eintritt. Sollte ein Paketverlust vorliegen, sendet das System eine E-Mail-Nachricht mit den Ergebnissen des Ping. Wenn es keinen Paketverlust gibt, wird das Ergebnis 'All OK' protokolliert.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Port Check

- **Port-Monitor 1**
  - Teil 1 von 2: Überwachen Sie einen Port an einem Host oder einer IP-Adresse und senden Sie eine E-Mail-Nachricht, wenn der Port nicht antwortet. Geben Sie in Schritt 1 den Hostnamen oder die IP-Adresse ein und dann in Schritt 2 die zu überwachende Portnummer. In Schritt 3 geben Sie die E-Mail-Adressen an (mehrere Adressen durch Kommata trennen), an die eine Warnung gesendet werden soll, wenn der Port nicht antwortet. Bearbeiten Sie das Verfahren 'Port Monitor 2', um den E-Mail-Betreff und -Textkörper zu ändern.
- **Port-Monitor 2**
  - Nehmen Sie KEINE Zeitplanung dieses Verfahrens vor. Es ist ein untergeordnetes Verfahren, das von Port Monitor 1 aufgerufen wird. Planen Sie die Ausführung von Port Monitor 1 auf einem Rechner, um einen Port an einem Host oder einer IP-Adresse zu überwachen.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Web Check

- **Web prüfen 1**
  - Das Verfahren ruft die Ausgabe der Webseite ab, die als Variable "siteURL" konfiguriert ist. Das Skript "Check Web 2" überprüft, ob der erwartete Inhalt in der Ausgabe vorhanden ist. Sie müssen die Variable "siteURL" und den Testdatei-Suchstring in "Check Web 2" konfigurieren, um dieses Verfahren anzupassen. Dieses Beispiel überprüft www.google.com/index.html auf das Wort "google".
- **Web prüfen 2**
  - Check Web 2 prüft, dass der erwartete Inhalt in der Ausgabe der URL-Anfrage vorhanden ist. Sie müssen den Inhalts des Testdatei-Befehls so ändern, dass er gefunden würde, wenn die getestete URL funktioniert. In diesem Beispiel prüfen wir auf das Wort "google" auf der Google-Homepage.

Core.4 Other Tools and Utility Procedures.Managed Services.Policy Management

- **Aktualisierung der Windows-Gruppenrichtlinie (GPUPDATE /FORCE)**
  - Lädt die Gruppenrichtlinie auf Windows-Rechnern neu.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Services Remediation

- **Service starten (W32Time)**
  - Dieses Verfahren startet den Windows-Zeitdienst neu. Dies ist ein Beispielverfahren, das zeigt, wie ein Dienst mit den Kaseya Agent-Verfahren gestartet wird.
- **Dienst anhalten (W32Time)**
  - Dieses Verfahren stoppt den Windows-Zeitdienst. Dies ist ein Beispielverfahren, das zeigt, wie ein Dienst mit den Kaseya Agent-Verfahren gestoppt wird.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Terminal Services

- **RDP-Überwachungsport für Terminaldienste ändern**
  - Dieses Verfahren ändert den Standard-RDP-Port für Terminaldienste von 3389 auf einen neuen Port Ihrer Wahl.

Core.4 Other Tools and Utility Procedures.Managed Services.System Management

- **SysInternals Process Explorer herunterladen**
  - Dieses Beispiel zeigt, wie Dateien von Remote-Quellen mit dem Befehl "Get URL" der Agent-Prozedur heruntergeladen werden. Geben Sie einfach die URL an, von der heruntergeladen werden soll, und den Zielspeicherort. In diesem Beispiel erfolgt das Herunterladen direkt von der Herstellerwebsite; eine beliebte Methode zur Dateiverteilung ist jedoch, die Dateien auf einer öffentlich zugänglichen FTP-Adresse oder einer Website (Cloud-Speicherung) zu speichern und sie so auf Ihre Endpunkte herunterzuladen. In diesem Beispiel wird die Datei einfach heruntergeladen; Sie können die Funktion aber auch auf das Installieren oder Ausführen von Dateien mithilfe von Shell-Befehl ausführen erweitern. Beachten Sie außerdem, dass wir in diesem Skript eine Variable für das temporäre Verzeichnis des Agent verwenden. Siehe **Pfad für Arbeitsverzeichnis des Agents** unter **Variablen verwenden** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2855.htm)* in der VSAOnline Hilfe.
- **Nachricht senden sofern angemeldet**
  - Dieses Verfahren sendet eine Nachricht an alle Benutzer, wenn Sie Wartungsaufgaben ausführen müssen. Auf einem System können Sie eine Nachricht über die Registerkarte für die Fernsteuerung senden, aber Nachrichten können nicht gesendet werden, wenn die Benutzer angemeldet sind.

Core.4 Other Tools and Utility Procedures.Operational Communications

- **OpComm-Meldungen kopieren**
  - Kopiert alle neuesten OpComm-Meldungsdateien vom Server auf den Zielrechner.
- **Benutzername abrufen – dann willkommen heißen**
  - Ruft den derzeit angemeldeten Benutzer aus einer SQL-Ansicht ab und sendet dann die Meldung "Willkommen bei unserem IT-Supportdienst" an diesen Benutzer. Wenn kein Benutzer angemeldet ist, plant sich die Agent-Prozedur neu, um 10 Minuten später erneut ausgeführt zu werden.
- **OpComm-ActionRequired**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "ActionRequired" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann

angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.

- **OpComm-Backup**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "Backup" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-Emergency**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "Emergency" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-MachineAudit**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "MachineAudit" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-MaintSchedule**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "MaintSchedule" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-NetworkDowntime**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "NetworkDowntime" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-PatchUpdate**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "PatchUpdate" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-RegularMaintenance**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "RegularMaintenance" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.

- **OpCommm-VirusScan**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "VirusScan" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-VirusThreat**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "VirusThreat" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.
- **OpComm-Welcome**
  - Zeigt dem angemeldeten Benutzer die OpComm-Meldung "Welcome" an. OpComm-Meldungen dienen der Kommunikation von Standardvorgängen, Benachrichtigungen und Erinnerungen. Der Ordner der OpComm-Meldungen kann angepasst und erweitert werden, um andere Arten der Endbenutzerkommunikation zu unterstützen. Diese Dateien befinden sich im Ordner Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm auf dem Kaseya Server.

Core.4 Other Tools and Utility Procedures.Patch Management

- **Status von WinAutoUpdate überprüfen**
  - Überprüft den letzten bekannten Status des automatischen Windows Update anhand des neuesten Patch-Scans und führt "WinAutoUpdate Enabled" aus, wenn dies aktiviert ist, oder "WinAutoUpdate Disabled", wenn dies deaktiviert ist. Wird zur Erstellung von Ansichten verwendet, die Rechner anzeigen, bei denen das automatische Windows Update aktiviert oder deaktiviert ist.
- **WinAutoUpdate Disabled**
  - FÜHREN SIE DIESES VERFAHREN NICHT AUS/PLANEN SIE ES NICHT. Es wird von "Status von WinAutoUpdate überprüfen" aufgerufen, wenn das automatische Windows Update auf einem Rechner deaktiviert ist.
- **WinAutoUpdate Enabled**
  - FÜHREN SIE DIESES VERFAHREN NICHT AUS/PLANEN SIE ES NICHT. Es wird von "Status von WinAutoUpdate überprüfen" aufgerufen, wenn das automatische Windows Update auf einem Rechner aktiviert ist.
- **Repository-Freigabe erstellen**
  - Erstellt den lokalen Dateiquellenordner und eine Netzwerkfreigabe, die als Repository für Windows-Patches dient, welche aus dem Internet mit Patch-Verwaltung heruntergeladen wurden.
- **Patch-Vorwarnung**
  - Sendet dem angemeldeten Benutzer eine Meldung, dass Patches und Sicherheitsaktualisierungen nun auf dem Rechner installiert werden. Es handelt sich hierbei um ein Verfahren, das vor automatischen Patch-Aktualisierungen durchgeführt wird.
- **Patch-Neustart**
  - Bei Windows-Arbeitsplatzrechner fordert das Verfahren den angemeldeten Benutzer zu einem Neustart auf, da Sicherheits-Patches/Aktualisierungen installiert wurden. Wenn ein Benutzer mit Ja antwortet, wird ihm mitgeteilt, dass sein System in einer Minute neu gestartet wird und er seine Arbeit speichern sowie seine Anwendungen schließen sollte. Antwortet der Benutzer mit "Nein", erscheint die Aufforderung zum Neustart nach 60 Minuten erneut. Ist kein Benutzer am Arbeitsplatzrechner angemeldet, wird das System neu

gestartet. Handelt es sich bei dem Rechner um einen Server und ist eine E-Mail-Adresse für den Patch-Neustart konfiguriert, so wird an die angegebene Adresse eine E-Mail mit dem Hinweis versendet, dass der Rechner aufgrund eines Neustarts die Aufmerksamkeit des Empfängers erfordert.

Core.4 Other Tools and Utility Procedures.Patch Management.Suspend Alarms After Patch

- **Unterbrechung der Alarme nach dem Patchen aufheben**
  - Hebt die Unterbrechung für monitoringbezogene Alarme auf. Es handelt sich hierbei um ein Verfahren, das nach automatischen Patch-Aktualisierungen durchgeführt werden sollte, wenn der jeweilige Rechner direkt nach dem Patchen neu gestartet wird.
- **Alarme für 10 Minuten unterbrechen**
  - Unterbricht monitoringbezogene Alarme für 10 Minuten. Es handelt sich hierbei um ein Verfahren, das nach automatischen Patch-Aktualisierungen durchgeführt werden sollte, wenn direkt nach dem Patchen ein Neustart erfolgt.
- **Alarme für 10 Minuten unterbrechen – wiederkehrend**
  - Unterbricht monitoringbezogene Alarme für 10 Minuten und aktiviert sich jedes Mal nach 5 Minuten erneut von selbst, damit keine Lücken im ausgesetzten Alarmintervall auftreten. Es handelt sich hierbei um ein Verfahren, das nach automatischen Patch-Aktualisierungen durchgeführt werden sollte, wenn möglicherweise nicht sofort ein Neustart erfolgt.
- **Alarme für 120 Minuten unterbrechen**
  - Unterbricht monitoringbezogene Alarme für 120 Minuten. Es handelt sich hierbei um ein Verfahren, das nach automatischen Patch-Aktualisierungen durchgeführt werden sollte, wenn nach dem Patchen nicht automatisch ein Neustart erfolgt.

Core.4 Other Tools and Utility Procedures.Run Now System Scripts

- **Jetzt ausführen – Basis-Audit**
  - Führt das Systemskripting "Basis-Audit" aus.
- **Jetzt ausführen – Automatische Windows-Aktualisierung deaktivieren**
  - Führt das Systemskripting "Automatische Windows-Aktualisierung deaktivieren" aus.
- **Jetzt ausführen – Aktuelles Audit**
  - Führt das Systemskripting "Aktuelles Audit" aus.
- **Jetzt ausführen – Patch-Scan**
  - Führt das Systemskripting "Patch-Scan" aus.
- **Jetzt ausführen – Serverrollenaudit**
  - Führt das clientseitige Benutzerkontensteuerungs-Systemskript zur Durchführung eines Serverrollenaudits aus.
- **Jetzt ausführen - Systeminformationen**
  - Führt das Systemskripting "Systeminformationen" aus.
- **Jetzt ausführen – Listen durch Scan aktualisieren**
  - Führt das Systemskripting "Listen durch Scan aktualisieren" aus.
- **Jetzt ausführen – Agent deinstallieren (Agent-Daten bleiben erhalten)**
  - Führt das Agent-Systemverfahren "Agent deinstallieren" aus. Nach der Deinstallation des Agents bleiben dessen Daten so lange im System erhalten, bis sie manuell gelöscht werden.
- **Jetzt ausführen – Automatische Windows-Aktualisierung zurücksetzen**
  - Führt das Systemskripting "Automatische Windows-Aktualisierung zurücksetzen" aus.

Monitor-Sets

Backup

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - Überwacht Backup Exec Continuous Protection Services auf Backup Exec-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - Überwacht Backup Exec DLO Agent Services auf Backup Exec Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - Backup Exec Services - {Severity3}**
  - Überwacht Backup Exec Services auf Backup Exec-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - Backup Exec System Recovery Service - {Severity3}**
  - Überwacht Backup Exec-Systemwiederherstellungs-Services auf Backup Exec-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - Überwacht BrightStor ARCServe Backup-Services auf BrightStor ARCServe Backup-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Datenbank

- **Database - SQL Server (All Instances) Services - {Severity3}**
  - Überwacht SQL Server Dienste auf SQL-Servern Dienste unter Verwendung des Wildcard MSSQL*-Dienstes. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server (Default Instance) - {Severity0}**
  - Sammelt SQL-Server (Standardinstanz)-Leistungsindikatoren auf SQL-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Database - SQL Server (Default Instance) Performance - {Severity2}**
  - Überwacht SQL-Server (Standardinstanz)-Leistung auf SQL-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Database - SQL Server (Default Instance) Services - {Severity3}**
  - Überwacht SQL-Server (Standardinstanz)-Dienste auf SQL-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2005 Optional Services - {Severity3}**
  - Überwacht SQL Server 2005-Dienste auf SQL Server 2005-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2005 Services - {Severity3}**
  - Überwacht SQL Server 2005-Dienste auf SQL Server 2005-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Database - SQL Server 2008 Optional Services - {Severity3}**

- Überwacht SQL Server 2008-Dienste auf SQL Server 2008-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

- **Database - SQL Server 2008 Services - {Severity3}**
  - Überwacht SQL Server 2008-Dienste auf SQL Server 2008-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

E-Mail

- **Email - Blackberry Server Performance - {Severity2}**
  - Überwacht die Blackberry Server-Leistung auf Blackberry-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Email - BlackBerry Server Services - {Severity3}**
  - Überwacht Blackberry Server-Dienste auf Blackberry-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2003 Services - {Severity3}**
  - Überwacht Exchange 2003-Dienste auf Exchange 2003-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2007 Services - {Severity3}**
  - Überwacht Exchange 2007-Dienste auf Exchange 2007-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**
  - Sammelt Leistungsindikatoren von Exchange 2010 Edge-Transport-Warteschlangen auf Exchange 2010-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  - Überwacht die Exchange 2010 Edge-Transport-Warteschlangenleistung auf Exchange 2010-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  - Überwacht die Exchange 2010 Edge-Transport-Warteschlangenleistung auf Exchange 2010-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange 2010 Services - {Severity3}**
  - Überwacht Exchange 2010-Dienste auf Exchange 2010-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange Client Active Logons - {Severity0}**
  - Sammelt Leistungsindikatoren aktiver Exchange Client-Logins auf Exchange-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - Überwacht den Exchange IMAP4-Dienst auf Exchange-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange POP3 Service - {Severity3}**

  - Überwacht den Exchange POP3-Dienst auf Exchange-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - Überwacht die Leistung von Exchange Server auf Exchange-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Email - Exchange Server (Core) Services - {Severity3}**
  - Überwacht die Exchange Server (Core)-Dienste auf Exchange Server (Core)-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - Sammelt Leistungsindikatoren von Exchange-Speichern und -Datenbanken auf Exchange-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Email - SMTP Queue Performance - {Severity3}**
  - Überwacht die SMTP-Warteschlangenleistung auf SMTP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Email - SMTP Server Service - {Severity3}**
  - Überwacht den SMTP-Serverdienst auf SMTP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Datei/Drucken

- **File / Print - DFS Service - {Severity3}**
  - Überwacht den DFS-Dienst auf DFS-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **File / Print - DFSR Service - {Severity3}**
  - Überwacht den DFSR-Dienst auf DFSR-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **File / Print - NTFRS Service - {Severity3}**
  - Überwacht den NTFRS-Dienst auf NTFRS-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
  - Überwacht die Leistung von Datei- und Druckservern bei Druckerwarteschlangen-Auftragsfehlern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **File / Print - Spooler Service - {Severity3}**
  - Überwacht den Spoolerdienst auf Datei- und Druckservern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Netzwerkinfrastruktur

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**

  - Überwacht Active Directory-Domänencontrollerdienste auf Active Directory-Domänencontrollern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Network Infrastructure - AD Domain Controller Performance - {Severity2}**
  - Überwacht die Active Directory-Domänencontrollerleistung auf Active Directory-Domänencontrollern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Network Infrastructure - DHCP Server Performance - {Severity2}**
  - Überwacht die DHCP-Serverleistung auf DHCP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Network Infrastructure - DHCP Server Service - {Severity3}**
  - Überwacht den DHCP-Serverdienst auf DHCP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Network Infrastructure - DNS Server Performance - {Severity2}**
  - Überwacht die DNS-Serverleistung auf DNS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Network Infrastructure - DNS Server Service - {Severity3}**
  - Überwacht den DNS-Serverdienst auf DNS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Network Infrastructure - WINS Server Service - {Severity3}**
  - Überwacht den WINS-Serverdienst auf WINS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Disk Space.Disk Space

- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - Überwacht den freien Festplattenspeicher auf allen Laufwerken mit weniger als 1 GB Speicher auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - Überwacht den freien Festplattenspeicher auf allen Laufwerken mit weniger als 2 GB Speicher auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - Überwacht den freien Festplattenspeicher unter 750 MB auf jedem Laufwerk auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk C von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk C von Windows-Rechnern, wenn jener unter 1 GB liegt. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**

- Überwacht den freien Festplattenspeicher auf Laufwerk C von Windows-Rechnern, wenn jener unter 750 MB liegt. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk D von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk E von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk F von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - Überwacht den freien Festplattenspeicher auf Laufwerk G von Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk C von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on C Drive Below 2GB - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk C von Windows-Rechnern, wenn weniger als 2 GB Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk D von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk E von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk F von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - Überwacht den freien Speicherplatz auf Laufwerk G von Windows-Rechnern, wenn weniger als 15 % Speicher verfügbar sind. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.

Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - Sammelt den Dienststatus für alle automatischen Dienste auf Windows-Rechnern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Windows (Core) - CPU and Memory - {Severity0}**

  - Sammelt Leistungsindikatoren von CPU und Speicher auf Windows-Rechnern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Windows (Core) - Machine Health - {Severity0}**
  - Sammelt Leistungsindikatoren zur Integrität von Windows-Rechnern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - Überwacht die Prozessor- und Speicherleistung auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  - Überwacht die TCPv4-Verbindungsleistung auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.

Windows-Server

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - Überwacht die Clusterdienste auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  - Überwacht die Leistung der Festplattenzeit und Warteschlangenlänge auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.
- **Windows Server (Core) - Drive C Performance - {Severity1}**
  - Überwacht die Leistung des Laufwerks C auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Server (Core) - General System Performance - {Severity1}**
  - Überwacht die allgemeine Systemleistung auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Server (Core) - Server Reboots - {Severity1}**
  - Überwacht die Server-Neustarts auf Windows-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Server (Core) - Standard Services - {Severity3}**
  - Überwacht die Standarddienste auf Windows-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server 2003 - Standard Services - {Severity3}**
  - Überwacht die Standarddienste auf Windows Server 2003-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server 2008 - Standard Services - {Severity3}**
  - Überwacht die Standarddienste auf Windows Server 2008-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Windows Server 2012 - Standard Services - {Severity3}**

  - Beschreibung: Überwacht die Standarddienste auf Windows Server 2012-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Windows-Arbeitsplatzrechner

- **Windows 7 - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows 7-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows 8 - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows 8-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows Vista - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows Vista-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.
- **Windows XP - Standard Services - {Severity1}**
  - Überwacht die Standarddienste auf Windows XP-Rechnern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad1" eingestuft.

Remotezugriff

- **Remote Access - Citrix Licensing Service - {Severity3}**
  - Überwacht den Citrix-Lizenzierungsdienst auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix Licensing WMI Service - {Severity3}**
  - Überwacht den Citrix-Lizenzierungs-WMI-Dienst auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix MetaFrame Services - {Severity3}**
  - Überwacht Citrix MetaFrame-Dienste auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix Server Services - {Severity3}**
  - Überwacht Citrix MetaFrame-Dienste auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**
  - Überwacht den Citrix-Dienst "Virtual Memory Optimization" (Optimierung des virtuellen Speichers) auf Citrix-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Terminal Server Services - {Severity3}**
  - Überwacht die Terminalserverdienste auf Terminalservern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Remote Access - Terminal Server Session Performance - {Severity2}**

  - Überwacht die Terminalserver-Sitzungsleistung auf Terminalservern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad2" eingestuft.

Sicherheit/Antivirus

- **AV - AVG Tech AVG Services - {Severity3}**
  - Überwacht AVG Tech-Virenschutzdienste auf Rechnern mit AVG Tech-Virenschutz. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - McAfee Enterprise Services - {Severity3}**
  - Überwacht McAfee Enterprise-Dienste auf Rechnern mit McAfee Enterprise. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Microsoft SE-FEP Services {Severity3}**
  - Überwacht Microsoft SE-FEP-Dienste auf Rechnern mit Microsoft SE-FEP. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Sophos Antivirus Services - {Severity3}**
  - Überwacht Sophos Antivirus-Dienste auf Rechnern mit Sophos Antivirus. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Symantec Antivirus Services - {Severity3}**
  - Überwacht Symantec Antivirus-Dienste auf Rechnern mit Symantec Antivirus. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Symantec Endpoint Protection Services - {Severity3}**
  - Überwacht Symantec Endpoint Protection-Dienste auf Rechnern mit Symantec Endpoint Protection. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Trend Micro Client Server Security Services - {Severity3}**
  - Überwacht Trend Micro Client Server Security-Dienste auf Rechnern mit Trend Micro Client Server Security. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **AV - Trend Micro OfficeScan Services - {Severity3}**
  - Überwacht Trend Micro OfficeScan-Dienste auf Rechnern mit Trend Micro OfficeScan. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Websysteme

- **Web Systems - FTP Server Service - {Severity3}**
  - Überwacht den FTP-Serverdienst auf FTP-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Web Systems - IIS Performance - {Severity3}**
  - Überwacht die IIS-Leistung auf IIS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Web Systems - IIS Server - {Severity0}**
  - Sammelt IIS-Server-Leistungsindikatoren auf IIS-Servern. Wird nur für die Monitor-Protokollanzeige und Reporting-Zwecke verwendet.

- **Web Systems - IIS Server Services - {Severity3}**
  - Überwacht die IIS-Serverdienste auf IIS-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.
- **Web Systems - SharePoint Server Services - {Severity3}**
  - Überwacht die SharePoint-Serverdienste auf SharePoint-Servern. Wird für die Monitor-Protokollanzeige, Reporting und Benachrichtigungszwecke verwendet. Alarme werden als "Schweregrad3" eingestuft.

Ereignis-Sätze

Sicherheit/Antivirus

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische McAfee Antivirus-Fehler- und Warnereignisse. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Microsoft Security Essentials/Forefront Endpoint Protection. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] AV - Microsoft SE-FEP (I) - SYS - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Informationsereignisse bezüglich Microsoft Security Essentials/Forefront Endpoint Protection. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - Überprüft die Anwendungs- und System-Ereignisprotokolle auf sonstige Antivirus-Fehler- und Warnereignisse. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - Überprüft die Anwendungs- und System-Ereignisprotokolle auf sonstige Antivirus-Informationsereignisse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse bezüglich Symantec/Norton AntiVirus. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse bezüglich Symantec/Norton AntiVirus. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse bezüglich Symantec/Norton AntiVirus. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Informationsereignisse bezüglich Symantec/Norton AntiVirus. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.

Backup

- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}**

  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Backup Exec. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in Backup Exec. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit fehlgeschlagenen/stornierten Aufträgen in Backup Exec. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit erfolgreich ausgeführten Aufträgen in Backup Exec. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in BrightStor ARCserve. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in BrightStor ARCserve. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse beim Backup von Microsoft Windows. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf sonstige spezifische Backup-Fehlerereignisse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf sonstige Backup-Informationsereignisse. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf sonstige spezifische Backup-Warnereignisse. Alarme werden als "Schweregrad1" eingestuft.

Datenbank

- **zz[SYS] Database - SQL Server (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.

- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische ACID-Ereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Backup-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Backup-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Backup-Ereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in den SQL Server-Datenbankressourcen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in den SQL Server-Datenbankressourcen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in den SQL Server-Datenbankressourcen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in den SQL Server-Datenbankressourcen. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Fehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.

- **zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte MSDTC-Ereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Netzwerkfehler- und Warnereignisse im Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Netzwerkfehler- und Warnereignisse im Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Abfragefehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Abfragefehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Replikationsereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Reportingfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Reportingfehler- und Warnereignisse in Zusammenhang mit SQL Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Reportingereignisse in Zusammenhang mit SQL Server. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**

- Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad1" eingestuft.

- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit Mehrfachinstanzen, die einen SQL Server-Agent betreffen. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit Einzelinstanzen, die einen SQL Server-Agent betreffen. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Informationsereignisse in Zusammenhang mit dem SQL Server-Cluster. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit SQL/mit dem Dienststeuerungsmanager. Alarme werden als "Schweregrad3" eingestuft.

E-Mail

- **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Warnereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Warnereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad2" eingestuft.

- zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Warnereignisse im Zusammenhang mit Blackberry Server. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit Exchange 2000 und 2003. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2000 und 2003. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2000 und 2003. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Exchange 2000, 2003 und 2007. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Ereignisse in Exchange 2007. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Clientzugriff in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Clientzugriff in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Clientzugriff in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Edge-Transport in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.

- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Edge-Transport in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse bezüglich Edge-Transport in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Hub-Transport in Exchange 2007 betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Hub-Transport in Exchange 2007 betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Hub-Transport in Exchange 2007 betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse, die das Postfach in Exchange 2007 betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse, die das Postfach in Exchange 2007 betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse, die das Postfach in Exchange 2007 betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Postfach in Exchange 2007. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Transportdiensten in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Transportdiensten in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Transportdiensten in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**

- Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Unified Messaging in Exchange 2007. Alarme werden als "Schweregrad1" eingestuft.

- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Unified Messaging in Exchange 2007. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Unified Messaging in Exchange 2007. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange 2010-Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange-Server. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Exchange-Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Informationsereignisse in Zusammenhang mit dem Exchange-Server. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Exchange Server 5.5. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Exchange/mit dem Dienststeuerungsmanager. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem SMTP/Dienststeuerungsmanager. Alarme werden als "Schweregrad3" eingestuft.

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**

  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Akku. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Akku. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Akku. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Akku. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Controller. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Controller. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Controller. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Controller. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Elektronik. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Elektronik. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Elektronik. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Dell-Elektronik. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Gehäuse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Gehäuse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Gehäuse. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Gehäuse. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**

- Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Umgebung. Alarme werden als "Schweregrad1" eingestuft.

- zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Umgebung. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Dell-Umgebung. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Dell-Umgebung. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Lüfter. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Lüfter. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Lüfter. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Lüfter. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit Änderungen an der Dell-Hardware. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Hardwareprotokoll. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Hardwareprotokoll. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}

  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Hardware-Protokoll. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Dell-Medien. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Dell-Medien. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit Dell-Medien. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit Dell-Medien. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit einem Vorausfall des Dell-Speichers. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit einem Vorausfall des Dell-Speichers. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSA-System. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSA-System. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSA-System. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-OMSA-System. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSM-System. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-OMSM-System. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}**

- Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der physischen Dell-Festplatte. Alarme werden als "Schweregrad1" eingestuft.

- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der physischen Dell-Festplatte. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der physischen Dell-Festplatte. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der physikalischen Dell-Festplatte. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Energiemanagement. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Energiemanagement. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Energiemanagement. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Energiemanagement. Alarme werden als "Schweregrad0" eingestuft.
- zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Prozessor. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit dem Dell-Prozessor. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit dem Dell-Prozessor. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Dell-Redundanzspiegelung. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Dell-Redundanzspiegelung. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}

  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Dell-Redundanzspiegelung. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Temperatur von Dell Geräten. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Temperatur von Dell Geräten. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der Temperatur von Dell Geräten. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Temperatur von Dell-Geräten. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der virtuellen Dell-Festplatte. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit der virtuellen Dell-Festplatte. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}**
  - Überprüft das System-Ereignisprotokoll auf spezifische Ereignisse in Zusammenhang mit der virtuellen Dell-Festplatte. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die HP Top Tools betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den HP/Compaq Insight Manager betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}**
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit dem HP/Compaq StorageWorks-Speicher. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}**
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische IBM SeriesX-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}**
  - Überprüft das System-Ereignisprotokoll auf sonstige Hardware-Fehlerereignisse. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}**

    - Überprüft das System-Ereignisprotokoll auf sonstige Hardware-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit sonstiger Hardware. Alarme werden als "Schweregrad1" eingestuft.

Netzwerkinfrastruktur

- **zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**
    - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**
    - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit Active Directory. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Audit-Ereignisse in Zusammenhang mit Fehlern bei Active Directory-Anmelde-/-Abmelde-/Sperraktivitäten. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit der Active Directory-NTDS-Datenbankdatei. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit der Active Directory-NTDS-Datenbankdatei. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
    - Überprüft das System-Ereignisprotokoll auf spezifische Active Informationsereignisse in Zusammenhang mit Active Directory. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit dem DHCP-Server. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf spezifische Warnereignisse, die den DHCP-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
    - Überprüft das System-Ereignisprotokoll auf spezifische Fehlerereignisse, die den DNS-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**

  - Überprüft das System-Ereignisprotokoll auf bestimmte Warnereignisse in Zusammenhang mit dem DNS-Server. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte Fehlerereignisse in Zusammenhang mit dem WINS-Server. Alarme werden als "Schweregrad1" eingestuft.

Remotezugriff

- zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit Citrix MetaFrame. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Citrix-Server-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Terminal-Server-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Terminal-Server-Fehlerereignisse. Alarme werden als "Schweregrad3" eingestuft.

Websysteme

- zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit IIS 6. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit IIS 7. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse in Zusammenhang mit IIS 7. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Fehlerereignisse, die den IIS-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}
  - Überprüft das Anwendungs-Ereignisprotokoll auf spezifische Warnereignisse, die den IIS-Server betreffen. Alarme werden als "Schweregrad1" eingestuft.

Betriebssystemplattformen

- zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Windows Server-Fehlerereignisse. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Windows Server-Fehlerereignisse. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Windows Server-Ereignisse. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}

- Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Fehler-Audit-Ereignisse. Alarme werden als "Schweregrad1" eingestuft.

- zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Fehler-Audit-Ereignisse. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Warnereignisse. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Windows Server-Warnereignisse. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}
  - Ignoriert die Überprüfung bestimmter, häufig auftretender Windows Server-Fehler- und Warnereignisse in den Anwendungs- und System-Ereignisprotokollen.
- zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Druck-Spooler des Windows-Servers betreffen. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Dienststeuerungs-Manager des Windows-Servers betreffen. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf spezifische Fehler- und Warnereignisse, die den Dienststeuerungs-Manager des Windows-Servers betreffen. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf spezifische Informationsereignisse, die den Dienststeuerungs-Manager des Windows-Servers betreffen. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}
  - Überprüft das System-Ereignisprotokoll auf Warnereignisse, die das Herunterfahren des Windows Server-Systems betreffen. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Fehlerereignisse bezüglich Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Fehlerereignisse bezüglich Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}
  - Überprüft das System-Ereignisprotokoll auf allgemeine Warnereignisse bezüglich Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}
  - Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der erweiterten Version von Windows Server 2008. Alarme werden als "Schweregrad2" eingestuft.
- zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}

- ➢ Überprüft das Anwendungs-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der erweiterten Version von Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.

- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**
  - ➢ Überprüft das System-Ereignisprotokoll auf spezifische erweiterte Fehler- und Warnereignisse, die erweiterte Windows Server 2008-Funktionen betreffen. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**
  - ➢ Überprüft das System-Ereignisprotokoll auf spezifische erweiterte Fehler- und Warnereignisse, die erweiterte Windows Server 2008-Funktionen betreffen. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**
  - ➢ Überprüft das System-Ereignisprotokoll auf spezifische erweiterte Fehler- und Warnereignisse, die erweiterte Windows Server 2008-Funktionen betreffen. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**
  - ➢ Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der erweiterten Version von Windows Server 2008. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**
  - ➢ Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**
  - ➢ Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**
  - ➢ Überprüft das System-Ereignisprotokoll auf bestimmte Fehler- und Warnereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**
  - ➢ Überprüft das System-Ereignisprotokoll auf bestimmte Ereignisse in Zusammenhang mit der Basisversion von Windows Server 2008. Wird nur für Protokollierungs- und Reporting-Zwecke verwendet.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**
  - ➢ Überprüft das Sicherheits-Ereignisprotokoll auf Fehler-Audit-Ereignisse im Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad1" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**
  - ➢ Überprüft das Sicherheits-Ereignisprotokoll auf Fehler-Audit-Ereignisse im Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad2" eingestuft.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**
  - ➢ Überprüft das Sicherheits-Ereignisprotokoll auf Fehler-Audit-Ereignisse im Zusammenhang mit der Basisversion von Windows Server 2008. Alarme werden als "Schweregrad3" eingestuft.
- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**

- Überprüft das System-Ereignisprotokoll auf bestimmte, häufig auftretende Fehlerereignisse im Zusammenhang mit Windows-Arbeitplatzrechnern. Alarme werden als "Schweregrad1" eingestuft.

Inhaltsverzeichnis

A

B

C

D

E

F

H

I

M

N

O

P

R

S

U

V

W